Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2016-03

Migrating to the cloud: preparing the USMC CDET for MCEITS

McLauchlin, Matthew S.

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/48564

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MIGRATING TO THE CLOUD: PREPARING THE USMC CDET FOR MCEITS

by

Matthew S. McLauchlin

March 2016

Thesis Advisor: Glenn Cook
Second Reader: Richard Bergin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2016	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE
MIGRATING TO THE CLOUD: PREPARING THE USMC CDET FOR MCEITS

5. FUNDING NUMBERS

6. AUTHOR(S) Matthew S. McLauchlin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

This research examines the Marine Corps' implementation of its private cloud computing environment into its Enterprise Architecture. Specifically, this analysis reviews the challenges presented in migrating the USMC College of Distance Education and Training's (CDET) entire portfolio of IT applications to the Marine Corps Enterprise Information Services (MCEITS) cloud data center. This study explores the necessary modifications to CDET's applications and business processes to make the migration a success, and how the modifications may help CDET realize the intrinsic benefits of cloud computing.

The analysis begins by establishing an understanding of the MCEITS' hosting environment and CDET's system requirements. Next, a review of cloud migration models and lessons learned from a commercial migration case provide context for examining the migration of CDET's applications. After providing an understanding of CDET's current "As-Is" processes, the research focus is on applying the migration guidance to develop and propose "To-Be" processes for post-migration operations.

This research concludes that CDET will benefit from the migration, as MCEITS will become responsible for the maintenance and upkeep of the network operating systems, database management systems, and infrastructure, and for competing data backups. This frees CDET personnel to concentrate on the development of CDET's applications. Also, the migration will result in a more streamlined change and procurement processes for acquiring computing resources. However, CDET will need to create new processes to facilitate coordination between the organizations.

14. SUBJECT TERMS
USMC, College of Distance Education and Training, MCEITS, CDET, cloud computing, public cloud, hybrid cloud, private cloud, Infrastructure as a Service, Platform as a Service, Software as a Service, cloud migration

15. NUMBER OF PAGES 139

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MIGRATING TO THE CLOUD: PREPARING THE USMC CDET FOR MCEITS

Matthew S. McLauchlin
Lieutenant Commander, United States Navy
B. S., Virginia Tech, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
March 2016

Approved by: Glenn Cook
Thesis Advisor

Richard Bergin
Second Reader

Dan Boger, PhD
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research examines the Marine Corps' implementation of its private cloud computing environment into its Enterprise Architecture. Specifically, this analysis reviews the challenges presented in migrating the USMC College of Distance Education and Training's (CDET) entire portfolio of IT applications to the Marine Corps Enterprise Information Services (MCEITS) cloud data center. This study explores the necessary modifications to CDET's applications and business processes to make the migration a success, and how the modifications may help CDET realize the intrinsic benefits of cloud computing.

The analysis begins by establishing an understanding of the MCEITS hosting environment and CDET's system requirements. Next, a review of cloud migration models and lessons learned from a commercial migration case provide context for examining the migration of CDET's applications. After providing an understanding of CDET's current "As-Is" processes, the research focus is on applying the migration guidance to develop and propose "To-Be" processes for post-migration operations.

This research concludes that CDET will benefit from the migration, as MCEITS will become responsible for the maintenance and upkeep of the network operating systems, database management systems, and infrastructure, and for competing data backups. This frees CDET personnel to concentrate on the development of CDET's applications. Also, the migration will result in a more streamlined change and procurement processes for acquiring computing resources. However, CDET will need to create new processes to facilitate coordination between the organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. BACKGROUND OF CLOUD COMPUTING....1
B. RESEARCH QUESTIONS....1
1. Problem Statement....1
2. Purpose Statement....2
3. Research Questions....2
C. RESEARCH GOALS....2
D. THESIS ORGANIZATION....3

II. BACKGROUND....5
A. CLOUD COMPUTING DEFINITION....5
B. CLOUD COMPUTING SERVICE MODELS....6
1. Infrastructure as a Service....7
2. Platform as a Service....7
3. Software as a Service....8
4. Data as a Service....8
C. CLOUD COMPUTING DEPLOYMENT MODELS....8
1. Private Cloud....9
2. Community Cloud....9
3. Public Cloud....9
4. Hybrid Cloud....9
D. CLOUD COMPUTING ADOPTION....10
1. Benefits....10
2. Challenges....12
E. MARINE CORPS ENTERPRISE INFORMATION TECHNOLOGY SERVICES....15
1. Characteristics of MCEITS....15
2. Organization and Structure....17
3. Initial Service Offerings....18
F. MARINE CORPS COLLEGE OF DISTANCE EDUCATION AND TRAINING....18
G. MIGRATION CONCERNS....21

III. MIGRATION PROCESS REVIEW AND APPLICATION....23
A. THE SEVEN-STEP MODEL FOR MIGRATION....23
B. IAAS CASE STUDY LESSONS LEARNED....26
1. Observed Benefits....26

2. Identified Risks....27
C. MCEITS APPLICATION INCLUSION PROCESS STANDARD OPERATING PROCEDURE....28
1. Organization....29
2. Preparation Phase....30
3. Migration Planning Phase....31
4. Service Transition Phase....32
D. DISTANCE LEARNING NETWORK OPERATIONS CENTER PRE-MIGRATION STANDARD OPERATING PROCEDURES (AS-IS)....32
1. Security....33
a. Access Control–User Accounts Process....33
b. Incident Reporting and Handling Process....36
c. Compliance Reporting Process....38
2. Database Administrator Functions....41
a. Ad Hoc/Canned Reporting Process....41
b. Database/System Restore (Stage) Process....44
c. Database/System Restore (Production) Process....45
d. Monthly Backup Offsite Process....48
3. Hosting and Network....49
a. Change Request Process....49
b. Patch Management Process....52
c. LMS Release Management Process....54
d. Outage Scheduling Process....56
e. Unscheduled Outage Recovery Process....57
4. Administration....60
a. Tasking Process....60
b. Procurement Process....61
E. MOVING FORWARD....64

IV. RESEARCH AND ANALYSIS....65
A. DOCUMENTATION REVIEW AND INTERVIEWS....65
B. DISTANCE LEARNING NETWORK OPERATIONS CENTER POST MIGRATION PROCESS MODIFICATIONS (TO-BE)....68
1. Security....68
a. Access Control–User Accounts Process....69
b. Incident Reporting and Handling Process....72
c. Compliance Reporting Process....74
2. Database Administrator Functions....77
a. Ad Hoc/Canned Reporting Process....77

b. Database/System Restore (Zone A) 80
c. Database/System Restore Process (Production) 82
d. Monthly Backup Offsite Process 85
3. Hosting and Network 85
a. Change Request Process 86
b. Patch Management Process 88
c. LMS Release Management Process 91
d. Outage Scheduling Process 93
e. Unscheduled Outage Recovery Process 96
4. Administration 99
a. Tasking Process 99
b. Procurement Process 101
C. SUMMARY 104

V. CONCLUSION AND RECOMMENDATIONS 107
A. CONCLUSION 107
B. FINDINGS 108
1. Research Question 1 108
2. Research Question 2 109
3. Research Question 3 109
C. RECOMMENDATIONS 110
D. FUTURE RESEARCH 111

APPENDIX 113

LIST OF REFERENCES 115

INITIAL DISTRIBUTION LIST 119

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. MCEITS Capabilities Diagram 16
Figure 2. The PCCE design with the Three Instances of MCEITS 17
Figure 3. MarineNet Logical Network 20
Figure 4. The Seven-Step Model for Migration into the Cloud 24
Figure 5. The Iterative Seven-Step Model of Migration into the Cloud 24
Figure 6. Access Control–User Accounts Process 34
Figure 7. Incident Reporting and Handling Process 37
Figure 8. Compliance Reporting Process 39
Figure 9. Ad Hoc/Canned Reporting Process 42
Figure 10. Database/System Restore (Stage) 44
Figure 11. Database/System Restore Process (Production) 46
Figure 12. Change Request Process 50
Figure 13. Patch Management Process 52
Figure 14. LMS Release Management Process 54
Figure 15. Outage Scheduling Process 56
Figure 16. Unscheduled Outage Recovery Process 58
Figure 17. Tasking Process 60
Figure 18. Procurement Process 62
Figure 19. MCEITS Service Offerings 66
Figure 20. Proposed Access Control–User Accounts Process 70
Figure 21. Proposed Incident Reporting and Handling Process 73
Figure 22. Proposed Compliance Reporting Process 75
Figure 23. Proposed Ad Hoc/Canned Reporting Process 78
Figure 24. Proposed Database/System Restore (Zone A) Process 81
Figure 25. Proposed Database/System Restore Process (Production) 83
Figure 26. Proposed Change Request Process 86
Figure 27. Proposed Patch Management Process 89
Figure 28. Proposed LMS Release Management Process 91
Figure 29. Proposed Outage Scheduling Process. 94
Figure 30. Proposed Unscheduled Outage Recovery Process 97

Figure 31. Proposed Tasking Process 100
Figure 32. Proposed Procurement Process 102
Figure 33. Process Flow Guide 113

LIST OF TABLES

Table 1. The Access Control–User Accounts Process Step-by-Step Description 35

Table 2. The Incident Reporting and Handling Process Step-by-Step Description 37

Table 3. The Compliance Reporting Process Step-by-Step Description 40

Table 4. The Ad Hoc/Canned Reporting Process Step-by-Step Description..... 43

Table 5. The Database/System Restore (Stage) Step-by-Step Description 45

Table 6. The Database/System Restore Process (Production) Step-By-Step Description 47

Table 7. Monthly Backup Offsite Process Step-by-Step Description..... 48

Table 8. The Change Request Process Step-by-Step Description 51

Table 9. The Patch Management Process Step-by-Step Description..... 53

Table 10. The LMS Release Management Process Step-by-Step Description..... 55

Table 11. The Outage Scheduling Process Step-by-Step Description..... 57

Table 12. The Unscheduled Outage Recovery Process 59

Table 13. The Tasking Process Step-by-Step Description..... 61

Table 14. The Procurement Process Step-by-Step Description 63

Table 15. Proposed Access Control – User Accounts Process Step-by-Step Description 71

Table 16. Proposed Incident Reporting and Handling Process Step-by-Step Description 73

Table 17. Proposed Compliance Reporting Process Step-by-Step Description..... 76

Table 18. Proposed Ad Hoc/Canned Reporting Process Step-by-Step Description 79

Table 19. Proposed Database/System Restore (Zone A) Step-by-Step Description 81

Table 20. Proposed Database/System Restore Process (Production) Step-by-Step Description..... 84

Table 21. Proposed Change Request Process Step-by-Step Description..... 87

Table 22. Proposed Patch Management Process Step-by-Step Description 90

Table 23. Proposed LMS Release Management Process Step-by-Step Description 92

Table 24. Proposed Outage Scheduling Process Step-by-Step Description 95
Table 25. Proposed Unscheduled Outage Recovery Process..... 98
Table 26. Proposed Tasking Process Step-by-Step Description..... 100
Table 27. Proposed Procurement Process Step-by-Step Description 103

LIST OF ACRONYMS AND ABBREVIATIONS

AAR	After Action Report
AIP	Application Inclusion Process
C4	Command, Control, Communications, and Computers
CDET	College of Distance Education and Training
CMB	Configuration Management Board
CMT	Contract Management Team
COR	Contract Officer Representative
COTS	Commercial-off-the-shelf
CRQ	Change Request
CTO	Chief Technical Officer
DaaS	Data as a Service
DBA	Database Administrator
DBMS	Database Management System
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DIP	DIACAP Implementation Plan
DLNOC	Distance Learning Network Operations Center
DOD	Department of Defense
DOD CIO	Department of Defense Chief Information Officer
EIO	Engineering Infrastructure Overview
EITC	Enterprise Information Technology Center
HQMC C4	Headquarters Marine Corps Command, Control, Communications, and Computers
IaaS	Information as a Service
IT	Information Technology
JON	Job Order Number
LOA	Line of Accounting
MAGTF	Marine Air-Ground Task Force
MCEITS	Marine Corps Enterprise Information Technology Services
MCEN	Marine Corps Enterprise Network

MCIEN	Marine Corps Information Enterprise
MCNOSC	Marine Corps Network Operations and Security Center
MITSC	MAGTF IT Support Center
NIST	National Institute of Standards and Technology
PCCE	Marine Corps Private Cloud Computing Environment
PaaS	Platform as a Service
SAAR	System Authorization Access Request
SaaS	Software as a Service
SECNAV	Secretary of the Navy
SLA	Service Level Agreement
SOP	Standard Operating Procedure
TAR	Tool Access Request
USMC	United States Marine Corps

ACKNOWLEDGMENTS

I would like to thank those who directly helped me with the development of this thesis. Glenn Cook and Richard Bergin were two of the best advisers a student could have. I am grateful for their insight, encouragement, and guidance throughout this process. I would like to thank Maj. Mike Gavin, USMC, and Mr. Doug Shuman from CDET for sponsoring me and providing background material to begin this research. I would also like to express my gratitude to Mr. Mark Johnson, the MCEITS Services Integrated Product Team (IPT) Lead and Maj. Seth Gibson, USMC (Ret.), formerly assistant to the MCEITS Services IPT Lead, for agreeing to take time out of their busy schedules and allowing me to interview them. They demonstrated a genuine eagerness to answer all the questions I asked them about MCEITS, and I will always appreciate the patience they showed during the interview process.

I would also like to thank those who supported me during this endeavor. First and foremost, I would like to thank my beautiful, intelligent, and patient wife, Melissa, for her understanding during the times I had to work late and leave her to handle our two children, Logan and Olivia, by herself. I am grateful to my father-in-law and mother-in-law, Ron and Barbara, for all the times they agreed to help Melissa with the kids while I was busy with my school work. In addition, I want to thank my parents, Joe and Elaine, for always encouraging me to work hard and value education.

Finally, I would like to thank God for placing all these people in my life to help me in this endeavor. He has truly blessed me with wonderful family and friends and has provided for me everywhere I have gone in my life. I am sure He will continue to do so wherever the Navy chooses to send me.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND OF CLOUD COMPUTING

Since 2011, when the United States Chief Information Officer Vivek Kundra published the *Federal Cloud Computing Strategy*, the adoption of cloud computing has become a priority for chief information officers across the federal government. The purpose of the strategy is to discuss how cloud computing can address major issues in the federal government's current IT environment. Kundra (2011) stated that the current environment suffers from low asset utilization, fragmented resource demand, redundant systems, unmanageable environments, and long procurement times. In response to the federal government directive to adopt cloud computing, the Marine Corps has published its private cloud computing environment (PCCE), which established the Marine Corps Enterprise Information Services (MCEITS) as a program of record (Anderson, 2012). The goal of the MCEITS program is to use cloud computing technologies to enhance operational effectiveness and reduce total cost of IT ownership (Anderson, 2012). To understand how cloud computing can assist with these issues warrants a thorough examination of the characteristics and features of cloud computing.

B. RESEARCH QUESTIONS

1. Problem Statement

The USMC College of Distance Education and Training (CDET) is preparing to implement the Marine Corps' Cloud Computing strategy by migrating its entire portfolio of IT applications to the MCEITS data center. This action will require CDET to relinquish local control of its process servers, which may force CDET to restructure and reengineer its business processes. Possible affected areas may include, but are not limited to, the processes for installing and updating software, procuring computing resources, developing courses, maintaining of personnel training records, and providing for customer technical support. CDET needs to conduct a thorough examination of its IT applications, systems, and business processes to identify and mitigate potential challenges to the migration process.

2. Purpose Statement

The purpose of this research is to conduct a thorough examination for determining the feasibility and adaptability of CDET's operations to the MCEITS cloud computing environment. MCEITS is central to the Marine Corps Cloud Computing strategy and its goal is to provide "guidance for synchronizing current Marine Corps IT programs" (Anderson, 2012, p. 2). This analysis will ascertain whether the migration will require modifications to CDET's applications and systems and how those modifications will affect CDET's customers. Additionally, this research will include an assessment of how and to what extent the migration to MCEITS may cause CDET to modify its internal business processes. Finally, this research will focus on determining ways for CDET to reengineer its processes to fully leverage the proposed benefits that cloud computing offers.

3. Research Questions

This thesis will answer the following questions:

1. Will the migration to the MCEITS environment require modifications to CDET's IT applications and systems and if so, will those modifications affect CDET's customer service?
2. Will the migration to the MCEITS environment require any significant changes to CDET's internal business processes? If so, which processes?
3. How can the requisite changes to CDET's business processes allow it to fully realize the benefits of cloud computing?

C. RESEARCH GOALS

The intent of this research is to conduct an overview of CDET's current internal business processes and determine how the migration to the MCEITS hosting environment will affect those processes. The research will include a business process reengineering approach that provides a summary of the current "as-is" processes and pinpoint the areas of concern for the migration. After the identification of these areas of concern, the focus of the analysis will be to determine proposed changes to CDET's process that will become the "to-be" model. The purpose of the "to-be" model is to prepare CDET for what its post migration processes may look like and how those processes can benefit

CDET. Finally, the goal will be to use this research to develop recommendations to provide CDET with guidance to make the migration as smooth a process as possible.

D. THESIS ORGANIZATION

Chapter II is a discussion of cloud computing, MCEITS, and CDET. It describes cloud computing industry accepted definitions, service models, deployment models, and the general benefits and challenges of cloud computing adoption. The MCEITS discussion introduces the characteristics of MCEITS, its organization and structure, and describes its initial service offerings. Finally, the CDET discussion provides an understanding of the needs of the organization and its components.

Chapter III will provide an understanding of the research methods applied to the study of this migration. The chapter will begin with a description of the Seven-Step model that outlines an accepted process for cloud migration. Next, a case of a commercial migration case will provide lessons learned to include observed benefits and identified risks. The Seven-Step model and the case study will provide a foundation for reviewing the MCEITS Application Inclusion Process (AIP). Finally, the chapter will end with discussion of CDET's Distance Learning Network Operations Center (DLNOC) pre-migration standard operating procedures (SOPs) that will act as the "as-is" processes to be analyzed. The discussion will provide the questions for each that will act as the basis for interviewing MCEITS personnel to determine required changes to the DLNOC SOPs.

Presented in Chapter IV will be the result of the interviews with MCEITS personnel and the answers to the questions from Chapter III. The answers will provide the basis for making alterations to the DLNOC SOPs that will become the proposed "to-be" processes for post-migration.

Chapter V will contain a summary of the research along with conclusions and recommendations. The recommendations will include opinions on how to embrace cloud computing, develop methods for making the migration process easier, and conduct future research opportunities.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. CLOUD COMPUTING DEFINITION

Cloud computing is a broad term that encompasses many aspects of modern telecommunications technology. Cloud computing is a disruptive concept that is both an innovative technology and a pioneering business model (Mohan, 2011). The "cloud" in cloud computing is a reference to early diagrams of computer networks using a picture of a cloud to represent the Internet (Rittinghouse & Ransome, 2010). Cloud computing describes the ability for companies or organizations, called cloud service providers, to provide customers access to their IT network hardware and software via the Internet (Armbrust et al., 2009). Specifically, the National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011, p. 3).

Cloud computing requires the provision of five essential services (Mell & Grance, 2011). NIST defined these five services as:

1. On-demand self-service. A customer is able to "obtain computing capabilities, such as server time and network storage, as needed" from the service provider with minimal human interaction (Mell & Grance, 2011, p. 3).
2. Broad network access. Customers access the computing resources over a network, usually the Internet, via various client applications with heterogeneous platforms at the customers' sites (Dillon, Wu, & Chang, 2010).
3. Resource pooling. The cloud service provider offers its customers computing capabilities by allocating and deallocating physical and virtual resources from the data center's pool of resources (Mell & Grance, 2011). This pool-based computing paradigm allows the cloud service provider to maximize efficiency through economies of scale (Dillon et al., 2010). A resultant effect of resource pooling is that the customer will have little to

"no control or knowledge over the exact location of the provided resources" (Mell & Grance, 2011, p. 3).

4. Rapid elasticity. Cloud customers are immediately able to scale up to meet computing demand peaks and release computing capacity after the demand peaks subside (Dillon et al., 2010). To the customer, the cloud service provider's computing capabilities have the appearance of being infinite and are available in any quantity at any time (Mell & Grance, 2011).

5. Measured service. Cloud service providers implement the ability to measure, control, and account for the level of datacenter usage by its customers (Mell & Grance, 2011).

Some may still argue over other additional aspects of cloud computing not included in the NIST list above. Zhang, Lu, and Boutaba (2010) best summed up the reason for this disagreement when they wrote:

> The main reason for the existence of different perceptions of cloud computing is that cloud computing, unlike other technical terms, is not a new technology, but rather a new operations model that brings together a set of existing technologies to run business in a different way. Indeed, most of the technologies used by cloud computing, such as virtualization and utility-based pricing, are not new. Instead, cloud computing leverages these existing technologies to meet the technological and economic requirements of today's demand for information technology. (p. 8)

While cloud computing seems to be a new concept in information technology, it is in fact a combination of existing technologies and business models being used in new and innovative ways.

B. CLOUD COMPUTING SERVICE MODELS

There are different models for cloud computing that vary in the type of services provided. Four accepted models that are of particular interest to the DOD are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Data as a Service (DaaS) (Takai, 2012). A closer examination of each service model will provide an understanding of their value.

1. Infrastructure as a Service

Infrastructure as a Service (IaaS) is the simplest concept in that the vendor provides its customers remote access to its processing, storage, networking, and computing hardware (Mell & Grance, 2009). IaaS is the most successful cloud computing service offering to date (Mohan, 2011). In this model, customers maintain ownership and control over the applications and data while outsourcing the hosting operations and technical infrastructure management to the cloud service provider (Rittinghouse & Ransome, 2010). Cloud service providers utilize virtualization technologies to allow them to allocate and decompose physical resources in an ad-hoc manner (Dillon et al., 2010). In other words, virtualization allows a cloud service provider to create virtual servers within its data centers that it then allows its customers to use as part of their networks in the same manner as a physical server. Virtualization also allows multiple tenants to coexist on a cloud service provider's data center (Tsai, Sun, & Balasooriya, 2010). Such a model allows organizations to acquire and release computing resources as their operating tempos dictate (Armbrust et al., 2010). The IaaS model is ideal for organizations that want to retain administrative control over its network and applications but do not want the responsibility of maintaining the physical hardware of the network. Amazon Web Services and Microsoft Azure Infrastructure Services are examples of IaaS providers (Olavsrud, 2015).

2. Platform as a Service

In the Platform as a Service (PaaS) service model, the vendor provides the working environment (operating system and development tools) for customers to generate their own applications (Yoo, 2011). PaaS is the preferred cloud service model for programmers who seek to develop web-applications that are independent of a specific operating system (Mohan, 2011). Under the PaaS model, the service provider must provide the platform for completed and in-progress applications as well as tools, libraries, and configuration management (Dillon et al., 2010). Google AppEngine is an example of PaaS (Dillon et al., 2010).

3. Software as a Service

NIST described SaaS as a model of cloud computing where the service provider offers its customers fee-based access to its software applications via some thin-client interface (Mell & Grance, 2009). This is in contrast to the traditional Software-as-a-Product model, where the customer purchases and installs software on personal computers (Rittinghouse & Ransome, 2010). The SaaS model saves the customer from having to deal with software installation, configuration, deployment and maintenance because these issues would be the responsibility of the cloud service provider (Tsai et al., 2010). The model also provides the customers with hardware savings. Since the software is running on the cloud service provider's hardware, the customer can use lower-end, lower cost machines with a thin-client interface. Google Mail and Google Docs are examples of SaaS cloud providers (Dillon et al., 2010).

4. Data as a Service

DaaS is a relatively new service model to cloud computing. In fact, DaaS is not currently defined in NIST Special Publication 800–145, *The NIST Definition of Cloud Computing* (Mell & Grance, 2011). The intent behind DaaS is to develop a method of handling data taken from diverse and dissimilar sources, such as transactional databases, data warehouses, enterprise resource planning (ERP) systems, and customer relationship management (CRM) solutions, and feed the data to a central location to aggregate, standardize, and enrich it for future use (Sheldon, 2014). The DOD's interest in DaaS stems from the model's ability to standardize data interfaces and to incorporate "big data" technologies while dynamically allocating resources for large data storage (Takai, 2010). DaaS has the potential to allow all authorized users to access the DOD's rapidly increasing data and provide them the means to turn that data into useable information (Takai, 2010).

C. CLOUD COMPUTING DEPLOYMENT MODELS

There are four accepted deployment models for how organizations implement and incorporate cloud computing into their enterprise architecture (Mell & Grance, 2011). The accepted models are detailed in the following subsections.

1. Private Cloud

A private cloud is an implementation of cloud computing where an organization establishes, or hires a contractor to establish, a datacenter for its sole utilization (Mell & Grance, 2011). The benefit of a private cloud is that the organization can maintain greater control over the cloud service, including security measures and mission-critical activities (Dillon et al., 2011). The disadvantage of such a solution is that the organization retains capital and operational costs since the organization owns and operates the infrastructure. Organizations adopting this model must weigh the benefits and costs to determine that private ownership is preferred.

2. Community Cloud

A community cloud is similar to a private cloud except the services are for the exclusive use of a community instead of a single organization. For this model, a community is a group of organizations that share the cloud infrastructure along with policies, requirements, values and concerns (Dillon et al., 2011). The decisions regarding the operation policies and cost sharing is determined democratically by the organizations in the community (Dillon et al., 2011).

3. Public Cloud

The term “public cloud” refers to a cloud service provider who offers its cloud infrastructure to the general public (Mell & Grance, 2011). Public Clouds are usually “made available in a pay-as-you-go manner” and the service itself is sometimes described as “utility computing” (Armbrust et al., 2009, p. 1). Unlike a private cloud, a public cloud service provider owns the datacenter and establishes the rules for its usage (Dillon et al., 2011).

4. Hybrid Cloud

NIST defines a hybrid cloud as “a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability” (Mell & Grance, 2011, p. 3). An organization that chooses to implement the

hybrid cloud model does so to optimize its resources by outsourcing its peripheral business functions to an external cloud provider while keeping its core competencies and sensitive data on its own private cloud (Dillon et al., 2011).

D. CLOUD COMPUTING ADOPTION

As with any new business concept or technology, cloud computing incites both optimism and concern for organizations seeking its adoption. The benefits of cloud computing have an enormous upside, which explains the federal government and DOD's desire for its incorporation into the enterprise architecture. However, there remains concerns that require addressing prior to any cloud migration efforts. For this reason, these benefits and challenges warrant closer inspection.

1. Benefits

Cloud computing is attractive to the federal government because it promises to make IT a utility or commodity with the ability modify capacity dynamically based on usage needs (Kundra, 2011). Rittinghouse and Ransome (2010) listed the following features of cloud computing that contribute to this utility view:

1. Reduced costs. The cloud computing service provider accepts the costs of building and maintaining the IT infrastructure.
2. Mobility for the workforce. Using Internet-based IT services allows organizations to move from location to location with greater ease.
3. Flexibility and scalability. Cloud computing allows the customer organization can request changes to its IT service as its needs require.
4. Quick IT implementation. By using a cloud service provider, a young organization can build its IT department with little lead time.
5. Transformation of the organization's IT department. Since the cloud service provider is responsible for implementation and maintenance of the IT infrastructure, the organization's internal IT personnel can focus on supporting the organization's core business functions and needs.
6. "Greening" of the data center. Cloud computing allows for the elimination of redundant equipment which provides for cost savings through lower energy consumption.

7. Access to high-performance applications for small/medium-sized businesses. Cloud service providers offer access to more advanced technologies and software on a utility basis that were previously unaffordable to small and medium-sized businesses.

The DOD perceives these characteristics as highly beneficial to its mission. The reduced implementation costs and flexible and scalable infrastructure would eliminate the need for end users to determine their exact computing needs prior to implementation (Kundra, 2011). This is especially useful with helping organizations within the DOD to avoid the sometimes long acquisition process for purchasing IT equipment that can take several months (Kundra, 2011). Cloud computing would allow an organization to request an initial IT capability and then expand or contract that capability as the organization determines its needs.

The "greening" of the data center is another important concept for cost savings in the federal government. As discussed by former DOD CIO, Teresa Takai (2012), cloud computing is a key for the DOD to overcome the "duplicative, costly and complex IT infrastructures" built by the service components over the years (p. 1). As Kundra (2011) pointed out, most federal agencies servers and data centers are running at less than 30 percent capacity. These servers and data centers consume power despite under usage. Cloud computing provides the roadmap for data center consolidation that will result in equipment, facility, and operational cost savings (Takai, 2012).

Using cloud computing provides other benefits to ensure better network operation for the DOD. From a security perspective, the resulting data center consolidation will afford the DOD the opportunity to streamline security by shrinking its network attack surface (DOD CIO, 2013). Cloud computing also allows for the development of production-representative environments for testing and evaluation without the cost of providing additional IT infrastructure (Kundra, 2011). This ability in cloud computing to create a virtual test network will allow application development teams to safely test software applications and patches prior to their integration into the active network.

2. Challenges

Despite the numerous potential benefits, there still exists numerous challenges to cloud computing adoption by the DOD. For example, the DOD's Joint Information Environment (JIE) implementation strategy (DOD CIO, 2013) mentioned the following challenges to cloud computing adoption:

1. Giving the DOD real-time visibility of all cloud activities which will require customer commands to surrender physical control over their systems.
2. Establishing a continuous monitoring system.
3. Designing intrusion detection, diagnosis and response processes.
4. Managing agile cloud service acquisition and funding.
5. Migrating and managing large amounts of data.
6. Mitigating the challenge of providing network access to tactical edge users.

Each of these challenges requires further analysis and mitigation before cloud computing can become a viable part of any DOD enterprise architecture.

The first major challenge to overcome with cloud computing is the acceptance by organizations to give up local control of their data and network. As new DOD CIO Terry Halvorsen (Kenyon, 2014) stated, the greatest challenge in promoting the new DOD cloud policy is convincing the services' data owners to physically "let go" of the data they are hoarding. This desire to maintain strict control over data can explain the appeal of the private cloud model. Private clouds allow organizations to have greater control over their data; however, building private cloud datacenters can cost just as much, if not more, than traditional server networks (Zhang et al., 2010).

Another mitigation requirement for organizations looking to migrate to the cloud is the implementation of continuous monitoring. Organizations must ensure constant access to its applications and data, which may be challenging. Under a cloud computing paradigm, an organization has to place its trust with cloud service providers who can commit to high quality of service and availability (Marston, Li, Bandyopadhyay, Zhang,

& Ghalsasi, 2011). This is especially important since customer care and quality of service are at the mercy of the cloud service provider and not at the control of the organization's internal IT support staff (Khajeh-Hosseini, Greenwood, & Sommerville, 2010). This demonstrates the importance of establishing and enforcing Service Level Agreements (SLAs) with cloud service providers.

Due to cloud computing's open, Internet accessible nature, intrusion detection and cyber security must be a major point of focus for the organization and the cloud service provider. As previously mentioned, a primary benefit of cloud computing for the DOD is the potential for data center consolidation. While this does hold the potential to allow for the concentration of cyber security efforts, it is also a double-edged sword since the cloud data center will become the target of hackers and cyber attackers. As a result, cloud service providers must address the following areas against network intrusion: (1) protect the data during upload to prevent hijacking; (2) store the data with encryption at all times; and (3) control access to the data (Marrow, 2011). The implementation of intrusion detection schemes and cyber security becomes more complicated by the fact that two entities (the originating organization and the cloud service provider) must coordinate their network protection strategies.

Agile acquisition of service and sustainment funding refers to the DOD's component services having to change their IT acquisition processes. Kundra (2011) pointed out that the federal government has previously purchased commodities like IT "in a fragmented, non-aggregated fashion—like a federation of small businesses" instead of a single entity (p. 28). Takai (2012) stated that the intention of the DOD's cloud computing strategy is to encourage the component services to "use or provide cloud services offered by other Components, other entities in the Federal Government, mission partners and commercial vendors that meet their specific mission requirements" (p. E-2). This objective change in acquisition process represents a substantial shift in the way the DOD traditionally does business.

Application and data migration strategy is perhaps the greatest challenge for incorporating cloud computing into the enterprise architecture. Some applications may not be suitable for cloud migration as is, and may need to modification in order to interact

with other cloud-based applications (Marston et al., 2011). In addition, some applications cannot be used in a cloud environment. Mohan (2011) described the challenge of migrating applications to the cloud with the following equation:

$$P \rightarrow P'_C + P'_L \rightarrow P'_{OFC} + P'_L$$

In the equation above, P represents the pre-migration state of a process or application. The middle equation represents the state of an organization's applications after its initial migration to the cloud. P'_C is the application part that resides on the cloud and P'_L is the part that remains on an organization's local servers. The right equation shows the final state where applications are optimized for the cloud environment, represented by P'_{OFC}. Processes or applications that can be completely migrated to the cloud will have a P'_L that is null (Mohan, 2011). However, some applications may require parts that are kept and maintained on local servers. The interactions between local servers and the cloud will pose a great technological and procedural challenge for the organization (Marston et al., 2011).

For cloud computing to work within the DOD, network access for the end users becomes a higher priority. Marston et al. (2011) explained networks utilizing cloud computing can have their services interrupted and data compromised by hardware or software failures, natural disasters, or malicious terrorist or criminal activities. Cyber-attacks are particularly concerning since the cloud computing data center can become the single point of failure for the enterprise, which in turn can expose the network to distributed denial of service (DDOS) attacks (Armbrust et al., 2009).

One additional issue with cloud migration that was not mentioned by the JIE strategy is the effect of cloud computing adoption on local IT staff. Many IT staffers may see the adoption of cloud computing as a threat to their jobs and their office culture (Marston et al., 2011). Due to surrendering the actual physical network to the cloud, the local IT professionals may begin to see their role as changing from *provider to certifier, consultant and arbitrator* (Yanosky as cited in Khajeh-Hosseini et al., 2010). Therefore, the cloud migration strategy must include gaining an understanding and adequately

addressing the local IT staff's perception of the benefits, risks, opportunities and concerns regarding the process (Khajeh-Hosseini et al., 2010).

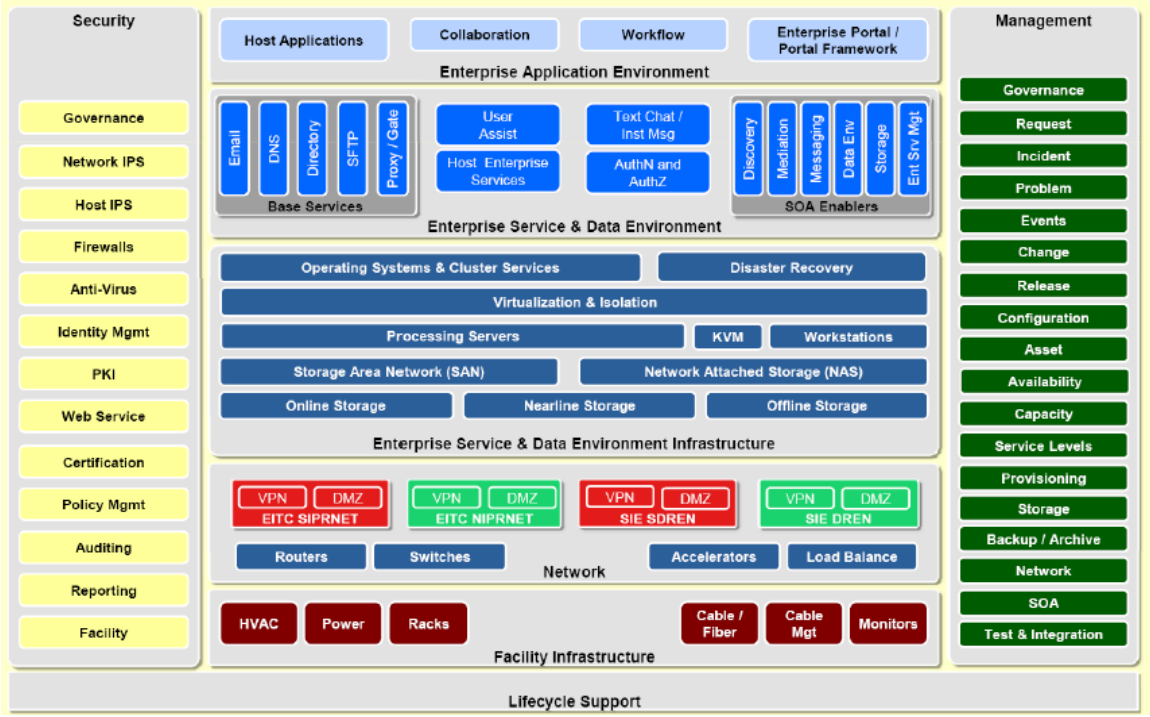
E. MARINE CORPS ENTERPRISE INFORMATION TECHNOLOGY SERVICES

In response to the federal cloud computing instruction, the Marine Corps has chosen to implement a private cloud computing strategy. The goal of the Marine Corps Private Cloud Computing Environment (PCCE) is to provide access to Marine Corps information and applications via "a shared pool of configurable resources…that can be provisioned and released with minimal management effort (Anderson, 2012, p. 1)." The PCCE is comprised of two parts, the Marine Corps Enterprise Network (MCEN) and the Marine Corps Enterprise Information Technology Services (MCEITS) (Anderson, 2012). The MCEN is the Marine Corps' network of networks and Program of Record that provides the physical IT infrastructure for connectivity (HQMC C4, 2014). The MCEITS program is responsible for building and maintaining the Marine Corps' government owned/government operated (GO/GO) private cloud data centers (Anderson, 2012).

1. Characteristics of MCEITS

MCEITS is a program of record that provides a collaborative sharing environment for information services by integrating commercial-off-the-shelf (COTS) IT components to create a net-centric environment (HQMC C4, 2014; Davis & Olsen, n.d.). The DOD defines a net-centric environment as a "framework for human and technical connectivity and interoperability that allows DOD users and mission partners to share and protect information and make informed decisions" (Grimes, 2007, p. 1). MCEITS possesses all of the NIST described characteristics associated with a cloud service provider to include secure on-demand self-service, flexible broad network access, resource pooling, elasticity, and measured service (Anderson, 2012; Mell & Grance, 2010). The PCCE also requires that MCEITS provides IaaS, PaaS, and SaaS service models, as previously described (Anderson, 2012). Additional capabilities built in to the MCEITS program design are shown in Figure 1.

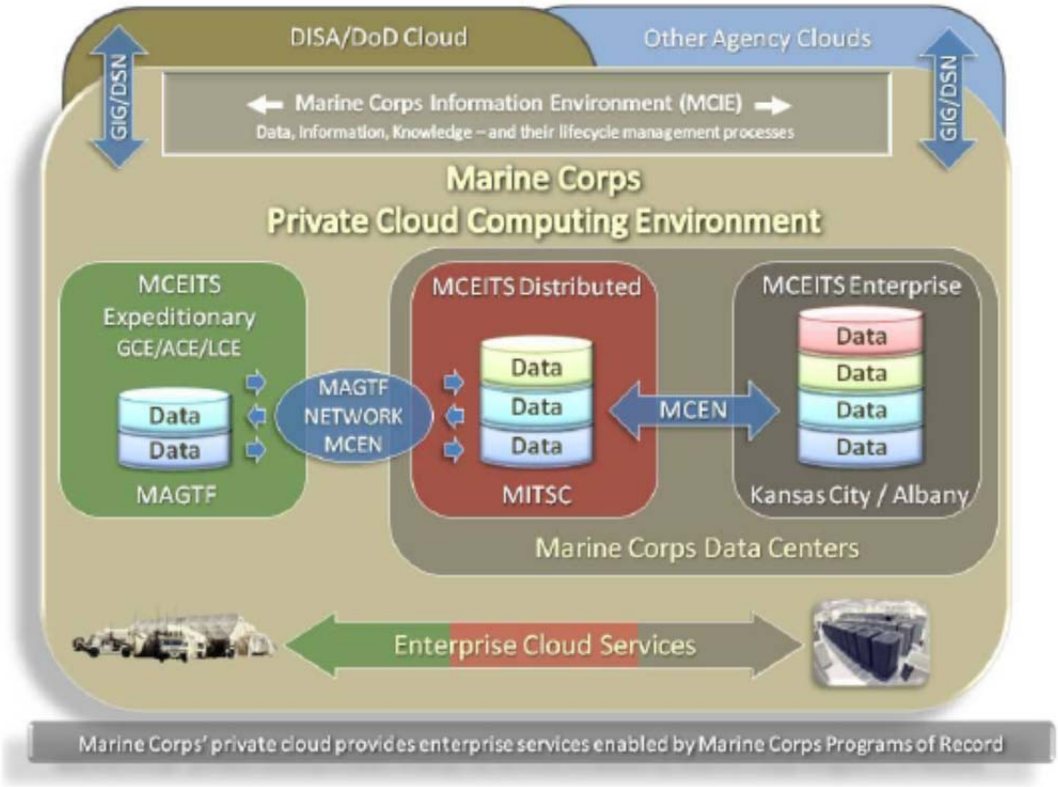
Figure 1. MCEITS Capabilities Diagram



Source: Anderson, R. (2012). Marine corps private cloud computing environment strategy. Arlington, VA: U.S. Marine Corps Headquarters.

Figure 2 represents the concept of the PCCE in which the MCEITS program provides a private cloud in three instances: Enterprise, Distributed, and Expeditionary (Anderson, 2012). The Distributed and Expeditionary instances of MCEITS will provide cloud computing services to forward deployed units in austere environments with limited bandwidth and connectivity (Anderson, 2012). These instances will synchronize with the Enterprise instance when greater connectivity becomes available (Anderson, 2012). However, this research involves the migration of a non-deployable data center and therefore will focus on the Enterprise instance of MCEITS.

Figure 2. The PCCE design with the Three Instances of MCEITS



Source: Anderson, R. (2012). Marine corps private cloud computing environment strategy. Arlington, VA: U.S. Marine Corps Headquarters.

2. Organization and Structure

The MCEITS program interacts with three Marine Corps commands—Marine Corps Systems Command (MARCORSYSCOM), Marine Corps Combat Development Command (MCCDC), and Headquarters, Marine Corps Command, Control, Communications, and Computers (HQMC C4). The MCEITS program office is subordinate to MARCORSYSOM as the acquiring command (Davis & Olsen, n.d.). MCCDC develops the requirements for the program (Davis & Olsen, n.d.). Scheduling the migration of customer commands to MCEITS is the responsibility of HQMC C4, which will also coordinate software IT standards with MCEITS (Colangelo, 2015). Service level agreements (SLAs) will define the relationship between MCEITS and the customer commands. The primary MCEITS data center is located in Kansas City,

Missouri, with a disaster recovery data center to be built at Camp Lejune, North Carolina (M. Johnson, telephone interview, November 20, 2015).

3. Initial Service Offerings

According to MARCORSYSCOM (Davis & Olsen, n.d.), the MCEITS design provides a common compliance environment that supports customer application migration with the following specifics:

1. Shared physical infrastructure
2. Standardized Enterprise Information Technology Service Management (E-ITSM)
3. Standardized configuration reporting
4. Support for architecture product (Operational View, Systems View, Technological View, All View) creation
5. Leverage MCEITS Information Assurance Type Accreditations
6. Common data storage

Currently, MCEITS is offering IaaS and PaaS with SaaS under development (Colangelo, 2015; M. Johnson, telephone interview, November 20, 2015). For the migration process, MCEITS will provide customer commands with a virtual private network (VPN), web access, server access, system administrator rights, database administrator rights and application administrator rights (Colangelo, 2015). The specifics of the service offerings will be part of the SLAs developed between MCEITS Application Inclusion Process (AIP) team and the customer commands (Colangelo, 2015).

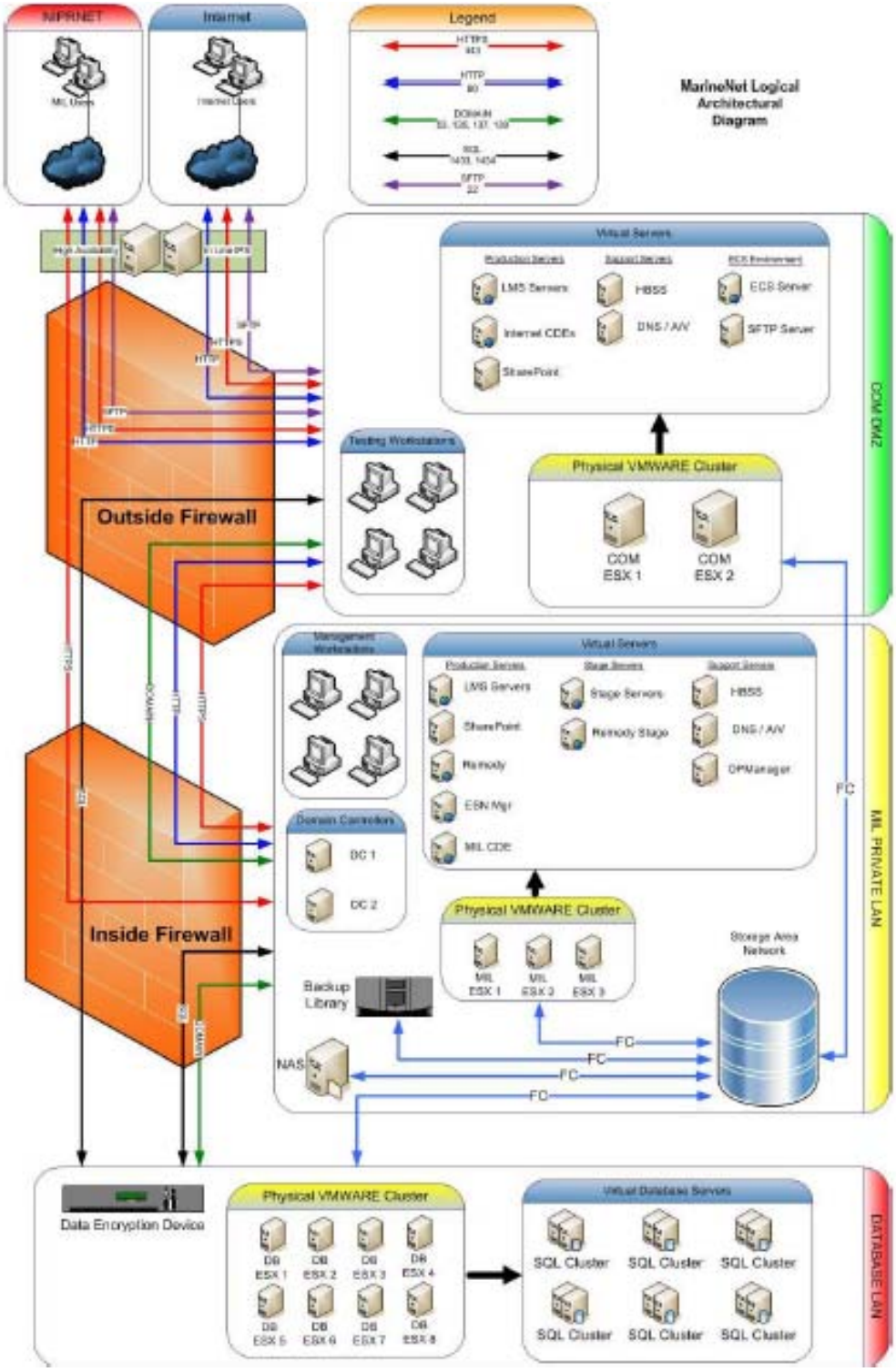
F. MARINE CORPS COLLEGE OF DISTANCE EDUCATION AND TRAINING

The College of Distance Education and Training (CDET) is part of the Marine Corps Training and Education Command (TECOM) and provides distance education opportunities for all Marines, government employees, and family members ("Welcome to CDET!", n.d.). As part of its mission, CDET must develop and deliver learning products *just-in-time* via such technologies as Interactive Multimedia Instruction (IMI), Video Teletraining (VTT) and Embedded Training (ET) in addition to traditional distance learning techniques such as correspondence courses and CD-ROM based instruction

(MCDLR, n.d.). The online learning management system of CDET is called the Marine Corps Distance Learning Network, or MarineNet (MITRE Corporation, 2000).

The Distance Learning Network Operations Center (DLNOC) is the data center that currently contains the hardware for MarineNet. Figure 3 shows a logical representation of the hardware within DLNOC (Mehl, 2013). For this thesis, the analysis will include the assumption that the migration will not begin until MCEITS has the means to meet all of CDET's technical requirements in accordance with Figure 3. The primary focus of this thesis will be an examination of the required changes to the DLNOC's standard operating procedures (SOP) are necessary upon completing the migration.

Figure 3. MarineNet Logical Network



Source: Mehl, B. (2013). MarineNet architecture design, version 1.0. St. Inigoes, MD: Naval Air Systems Command Special Communications Requirements Division.

G. MIGRATION CONCERNS

The MarineNet program is a major component in CDET's mission to provide distance learning opportunities to its customers (MITRE Corporation, 2000). The program's current design allows it to "effectively support Marines during annual training surges, increase program capabilities, leverage new technologies to conduct business, and position the system to support future needs of the USMC" (Mehl, 2013, p. 45). In preparation for MarineNet's migration from a traditional, locally maintained data center to the MCEITS hosting environment, CDET must ensure that the new implementation of MarineNet continues to possess the capabilities previously described. Therefore, a thorough review and understanding of the cloud migration process is warranted. This review is the focus of the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

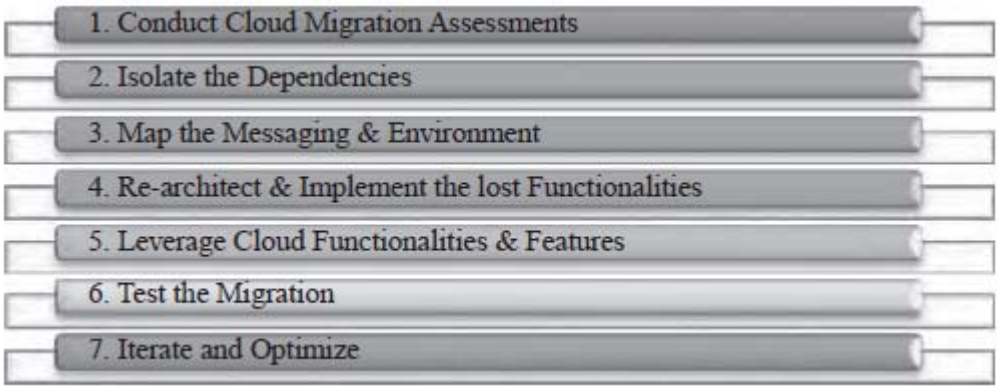
III. MIGRATION PROCESS REVIEW AND APPLICATION

This chapter covers the research methodology for examining the migration of the College of Distance Education and Training's (CDET) information technology (IT) enterprise to the Marine Corps Enterprise Information Technology Services (MCEITS) hosting environment. The first step will involve a review of the Seven-Step Model for Migration as discussed by Mohan (2010) in *Cloud Computing: Principles and Paradigms.* The next step will review a case study presented by Ali Khajeh-Hosseini et al. (2010) from the University of St. Andrews involving an IT solutions company migrating to Amazon's Elastic Compute Cloud (EC2) Infrastructure as a Service (IaaS) and the lessons learned from its migration. The first two steps will formulate the basis of the examination of the MCEITS Application Inclusion Process (AIP). The purpose of this examination is to pinpoint any unaddressed areas of concern in the MCEITS AIP. Finally, a review of the CDET Distance Learning Network Operations Center's standard operating procedures will identify the processes whose post migration status will be the focus of the research and analysis in Chapter IV.

A. THE SEVEN-STEP MODEL FOR MIGRATION

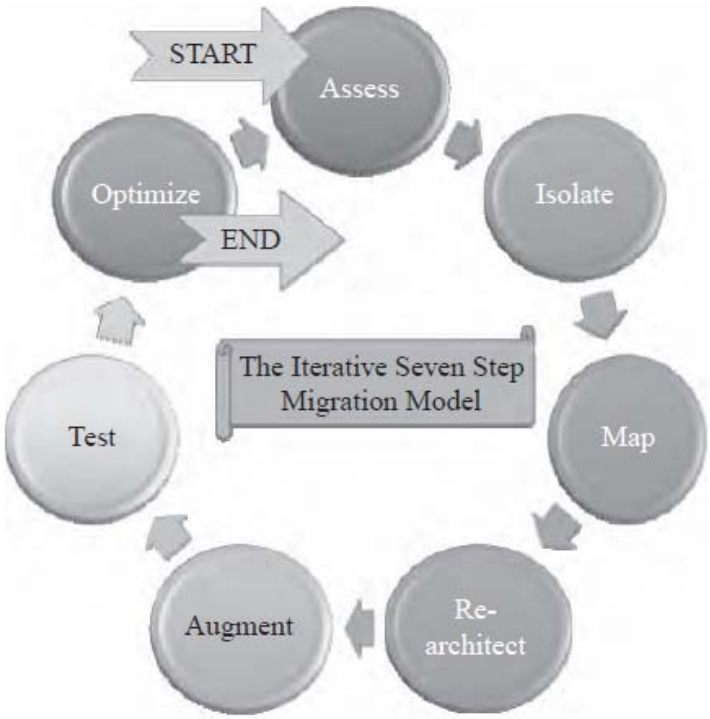
Mohan (2010) described a seven-step process for cloud migration that captured the best practices of many migration projects. The seven-steps of the model are (1) Assess, (2) isolate, (3) map, (4) re-architect, (5) augment, (6) test, and (7) optimize (Mohan, 2010). These steps are shown in Figures 4 and 5. The purpose of Figure 5 is to show that for larger migration efforts, the migration process by be iterative and require numerous repeating of the seven steps in phases to achieve completion.

Figure 4. The Seven-Step Model for Migration into the Cloud


1. Conduct Cloud Migration Assessments
2. Isolate the Dependencies
3. Map the Messaging & Environment
4. Re-architect & Implement the lost Functionalities
5. Leverage Cloud Functionalities & Features
6. Test the Migration
7. Iterate and Optimize

Source: As cited in Mohan, T. (2011). Migrating into a cloud. In R. Buyya, J. Broberg, & A. Goscinski, (Eds.), *Cloud computing: Principles and paradigms* (pp. 43–56). Hoboken, NJ: John Wiley & Sons.

Figure 5. The Iterative Seven-Step Model of Migration into the Cloud



Source: As cited in Mohan, T. (2011). Migrating into a cloud. In R. Buyya, J. Broberg, & A. Goscinski, (Eds.), *Cloud computing: Principles and paradigms* (pp. 43–56). Hoboken, NJ: John Wiley & Sons.

Understanding the Seven-Step Model requires an examination of what each step entails. Step 1, Assess, involves assessing the issues relating to migration at the

application, code, design, and architecture levels (Mohan, 2010). During this step, the migrating organization and the cloud service provider should assess the technical requirements for this migrated system. Mohan (2010) recommended the development of proof of concepts for migration to assure a proper assessment in this step.

The Isolate step of the migration model refers to isolating system dependencies within the current data center (Mohan, 2010). System dependencies refer to the relationship between applications, databases, and operating systems to include how they interact and depend on each other to function. The goal of this step is to fully determine the complexity of the migration (Mohan, 2010).

After the isolation of system dependencies, the third step is called Mapping. Mapping involves determining which applications to migrate to the cloud and which applications to retain on the current data center (Mohan, 2010). As previously discussed in Chapter II, some applications are not suitable for migration to the cloud and will remain on local servers. This step will also include determining the methods of interaction for the cloud applications and the locally maintained applications.

The migration process may require applications to be re-architected in order to work in a cloud environment (Mohan, 2010). During Step 4 (Re-architect), the migration team will implement the restructuring to the applications as needed. However, the re-architect step may affect the applications with some lost functionalities (Mohan, 2010).

The fifth step, Augment, involves adjusting the applications by using the features intrinsic to the cloud computing service (Mohan, 2010). The augmentation is done to improve the application and possibly address any lost functionality from the re-architecting.

The Test step consists of validating and testing the applications and proof-of-concepts (Mohan, 2010). The testing will include the use of an extensive test suite that will analyze the performance of the cloud applications (Mohan, 2010).

The seventh and final step of the model focuses on optimizing the post migration enterprise. Areas for optimization include addressing inefficiencies discovered during testing, improving compliance with standards and governance, maximizing the return on

investment for the migration, and developing a roadmap for leveraging new cloud features (Mohan, 2010). Industry best practices indicate optimization may take several iterations to achieve (Mohan, 2010).

B. IAAS CASE STUDY LESSONS LEARNED

In 2010, Khajeh-Hosseini et al. conducted a study on a United Kingdom based IT solutions company that serviced the Oil and Gas industry. The company migrated the IT infrastructure of three client companies to the cloud using Amazon EC2 (Khajeh-Hosseini et al., 2010). The authors' study consisted of six semi-structured interviews with employees of one of the client companies to determine the benefits and risks that resulted from the migration (Khajeh-Hosseini et al., 2010). Included in Khajeh-Hosseini et al.'s (2010) research was the following stakeholder analysis:

1. Identifying the stakeholders;
2. Identifying changes in what tasks they would be required to perform and how they were to perform them;
3. Identifying what the likely consequences of the changes are with regards to stakeholders' time, resources, capabilities, values, status and satisfaction;
4. Analyzing these changes within the wider context of relational factors such as tense relationships between individuals or groups to which stakeholders belong;
5. Determining whether the stakeholder will perceive the change as unjust (either procedurally or distributively) based upon changes and their relational context (p. 452).

Khajeh-Hosseini et al. recorded their observed benefits and identified the top perceived risks after conducting their interviews. The results of their work are discussed in the next sections.

1. Observed Benefits

Responses to the interview questions identified the following top five perceived benefits from the client company's migration to cloud computing:

1. Opportunity to better manage income and expenses. The employees found that the cloud infrastructure facilitated easing of cash-flow management since the cloud pricing model provided little upfront costs and monthly billing (Khajeh-Hosseini et al., 2010). As previously mentioned in Chapter II, the new pricing model essentially turns IT infrastructure costs into a utility cost model. This frees the client company of the burden of all the expenses associated with building and maintaining its own internal data center.
2. Improved status. Some employees reported that the migration provided them the opportunity to improve their status with the company by being supporting of management's cloud computing initiatives (Khajeh-Hosseini et al., 2010). The employees perceived cloud computing as a prestigious new technology that could provide a strong career progression (Khajeh-Hosseini et al., 2010).
3. Improve satisfaction of work. Employees of the client company reported to better liking their jobs. In particular, the IT support engineers stated that cloud computing freed them from the tedious and monotonous tasks associated with maintaining the network and generating data backups (Khajeh-Hosseini et al., 2010).
4. Opportunity to develop skills. Working with cloud computing technologies exposed IT support engineers to new and marketable skills that will be in demand for years (Khajeh-Hosseini et al., 2010).
5. Opportunity for organizational growth. As previously mentioned, a valued property of cloud computing is that it provides quick scalability in contrast to in-house data centers. This ability benefits the client company by allowing it to pursue sales targets and projects that it may not have attempted due to previous scalability limitations (Khajeh-Hosseini et al., 2010).

2. Identified Risks

The research of Khajeh-Hosseini et al. (2010) also uncovered some perceived risks that require address. The following concerns comprise the top five risks identified in their research.

1. Deterioration of customer care and service quality. IT support engineers expressed concern regarding their dependency on the cloud service provider to troubleshoot and fix hardware and network issues (Khajeh-Hosseini et al.,

2010). This will add complexity to the customer support process which, in turn, may diminish the support team's problem resolution rate.

2. Decrease in work satisfaction. Some IT personnel did not appreciate that they would no longer have a hands-on technical role on the network after completion of the migration (Khajeh-Hosseini et al., 2010). This could lead to a decrease in job satisfaction for those personnel who are resistant to change.

3. Departmental downsizing. IT support engineers showed concern that the company may downsize the IT department due to the decrease in workload after the migration (Khajeh-Hosseini et al., 2010). With the hardware and network support effectively outsourced to the cloud provider, the IT personnel worry that there will not be a large enough workload to justify current manning levels.

4. Uncertainty with new technology. Employees expressed concern that cloud computing may expose the company to "long-term volatility derived from market forces associated with the costs of using a cloud and data transfer costs" (Khajeh-Hosseini et al., 2010, p. 455). In addition, the employees worried that the migration may lead to an eventual loss of in-house hardware and networking expertise should the cloud service provider proves inadequate (Khajeh-Hosseini et al., 2010).

5. Lack of supporting resources. The research found there is a risk that the migration may require the temporary upsizing of the IT department due to the lack of knowledge and experience of the current team with cloud computing technology (Khajeh-Hosseini et al., 2010).

Khajeh-Hosseini et al. (2010) summarized that these risks demonstrated that organizational perspectives are just as important to the migration process as financial and technological aspects.

C. MCEITS APPLICATION INCLUSION PROCESS STANDARD OPERATING PROCEDURE

To provide guidance for migrating existing IT infrastructure to the MCEITS private cloud, the Marine Corps provided Operational Document OSS-210, *MCEITS Application Inclusion Process Standard Operating Procedure* (Schaefer, 2014). Outlined in OSS-210 is the Application Inclusion Process (AIP) whose purpose is to take a comprehensive look at the "hardware, software, Information Assurance (IA), and operational needs of an application and provides recommendations for migration"

(Schaefer, 2014). In addition, the document includes a description of the organizations involved in the process and the three phases of the migration—Preparation, Migration Planning, and Service Planning (Schaefer, 2014). The following sections will provide as closer review of each topic.

1. Organization

OSS-210 (Schaefer, 2014) provided for the creation of an AIP team to develop the migration plan for MCEITS's customer commands. According to the OSS-210 (Schaefer, 2014), the AIP team is to consist of the following members:

1. AIP Project Manager. The project manager ensures that all functions in each phase are completed and that the project maintains momentum.
2. IA Team. This team verifies that the migrating application has a current Authority to Operate (ATO)/Authority to Connect (ATC). This team works with the customer to bring the customer's IA standards in compliance with the MCEITS IA standards. Team members are the MCEITS IA Team, Kansas City (KC) MCEITS IA Team, Quantico AIP IA and Customer Information Assurance Manager (IAM).
3. Kansas City Integration/Engineering/Release Team. This team, comprised of technical SMEs (Subject Matter Experts), designs the "to-be" configuration of the application. The team members may include Enterprise Architects, Database Engineers, Storage Engineers, and Network Engineers. Specific team members are the KC AIP Engineer, the Quantico AIP engineer, and the KC Integration/Engineering Team.
4. Modeling and Simulation (M&S) Team. This team conducts the operational simulations for applications as they progress through the AIP. This team also provides performance monitoring results to the Kansas City Integration/Engineering Team for inclusion into the Request For Change (RFC) documentation and future planning.
5. Additional members from the customer organization include the following:
    a. Customer
    b. Application technical subject matter experts (SME)
    c. AIP Coordinator
    d. AIP Government Lead

e. Command, Control, Communications, and Computers (C4)

f. Systems Engineering, Interoperability, Architectures, and Technology (SIAT)

g. Engineering Review Board Charter Members

h. Release Planner

The AIP team's SMEs are to act as liaisons between the customer and the MCEITS entities and assist with migrating applications (Schaefer, 2014).

Other organizations that influence the process are Headquarters Marine Corps C4 (HQMC C4), Marine Corps Network Operations and Security Command (MCNOSC), and the MCEITS Operations Center (MOC) (Schaefer, 2014). HQMC C4's Information Technology Steering team approves changes to the migration schedule (Schaefer, 2014). The MCNOSC manages the hands on engineers and technicians at the Kansas City data center for the MCEITS production environment (Schaefer, 2014). The MOC monitors and manages the MCEITS production environment from Quantico, Virginia (Schaefer, 2014).

2. Preparation Phase

During the Preparation Phase, the AIP team begins the process of surveying the customer organization's infrastructure and applications to assess the magnitude of the impending migration. Specifically, Schaefer (2014) listed the following goals for the Preparation phase of the AIP:

1. Meet and establish a relationship with the customer.
2. Explain the hosting options and services within the Technical Service Catalog.
3. Make a determination on the application's suitability for migration.
4. Submit a Change Request (CRQ).
5. Plan an IA Strategy.
6. Develop initial Engineering Infrastructure Overview (EIO) and Service Level Agreement (SLA).
7. Provide EIO to MCEITS Engineering to complete the Integration Review.

8. Receive Host names and Internet Protocols (IPs) to begin Request for Modifications (RFM).
9. Provide guidance to the customer for the access management process (physical/logical).
10. Gather performance monitoring data and system information files.

The Preparation Phase of the AIP is the phase under which the first three steps of the Seven-Step Model of Migration (Conduct cloud migration assessments, Isolate the deficiencies, and Map the messaging and environment) occurs.

3. Migration Planning Phase

Under the Migration Planning Phase, the AIP team will address steps four and five of the Seven-Step Model of Migration (Re-architect/Implement the lost functionalities and Leverage cloud functionalities and features). The AIP team finalizes the technical details of the migration process by providing finalized documentation outlining the process. Schaefer (2104) detailed the goals of this phase in the following:

1. Assess the operational needs of a given application and facilitate integration of the application's IA controls into MCEITS IA controls.
2. Identify any gaps in services and develop a Plan of Action & Milestones (POA&M) to address those gaps.
3. Assist and support the required development/integration.
4. Establish a migration plan and develop/update the following documents: EIO, SLA, updated Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Implementation Plan (DIP), System Authorization Access Request/Tool Access Request and a CRQ.

Once an agreement for the migration exists with the approval of all documentation, the AIP team can then proceed to the Service Transition Phase of the process.

4. Service Transition Phase

The Service Transition Phase will complete the migration and address the final steps (Test the migration and Iterate and Optimize) of the Seven-Step Model of Migration. Schaefer (2104) described the following goals of this phase:

1. Finalize the Release Plan.
2. Complete the Zone A (Test) Build.
3. Verify the application's IA posture, functionality, and interoperability with MCEITS core services.
4. Complete service validation and testing on the test build.
5. Deploy the validated test build to the production environment.
6. Verify the application's IA posture, functionality, and interoperability within the MCEITS production environment.

Zone A is the term that MCEITS personnel use to for the MCEITS pre-production testing environment (Schaefer, 2014). The AIP team will conduct extensive testing in this environment prior to "going live" and completing the migration process.

D. DISTANCE LEARNING NETWORK OPERATIONS CENTER PRE-MIGRATION STANDARD OPERATING PROCEDURES (AS-IS)

Understanding the effects of the MCEITS migration on CDET's processes warrants an examination of CDET's current processes. While this thesis will be unable to scrutinize every CDET process, its examination will include a review of CDET's Distance Learning Network Operations Center (DLNOC) standard operating procedures (SOPs). More specifically, the research will focus on the procedures outlined in the *Distance Learning Network Operations Center Operations and Maintenance Standard Operating Procedure Version 1.0* (Booz Allen Hamilton, 2015).

The DLNOC Operations and Maintenance SOP describes the duties and processes of the DLNOC Operations and Maintenance Team (O&MT) with regards to four functional areas. Those functional areas include (1) Security; (2) Database functions; (3) Hosting and Network; and (4) Administration (Booz Allen Hamilton, 2015). The following sections will review the processes associated with each functional area, identify the actors in each process, and formulate questions that the research should address. The

DLNOC utilizes the Remedy service management system for tracking tasks and trouble tickets (Booz Allen Hamilton, 2015). The purpose of the later research will be to answer the formulated questions that cannot be answered directly by MCEITS documentation and will require further discussion during the interviews.

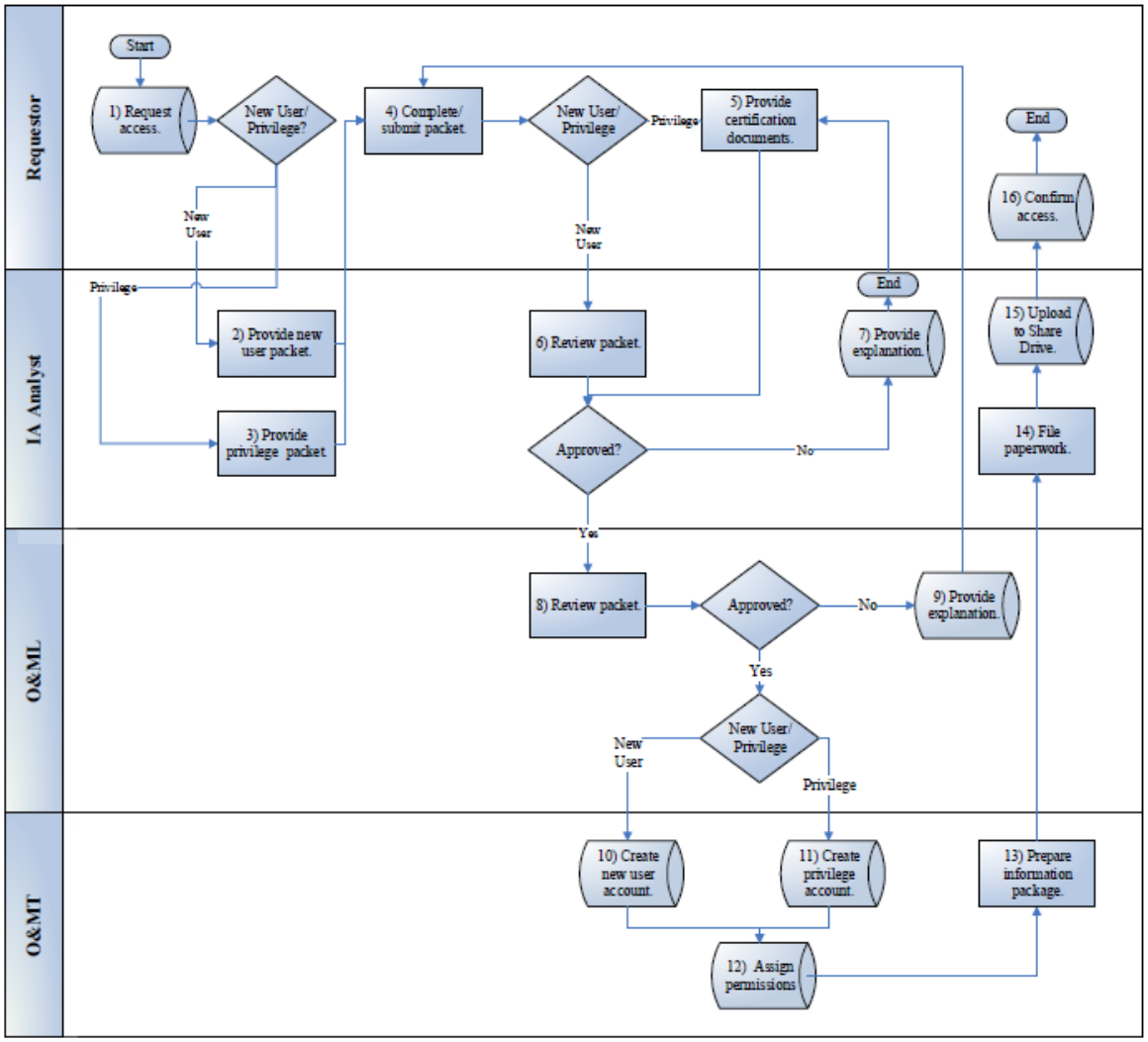
1. Security

The security function area focuses on the processes that provide access to MarineNet Learning Management System, responses to security incidents, and verification of compliance with security directives (Booz Allen Hamilton, 2015). In addition to the O&MT, the other actors for these security processes include the Information Assurance Analyst (IA Analyst), the Operations and Management Team Lead (O&ML), and the command Security Officer.

a. Access Control–User Accounts Process

The Access Control–User Accounts Process provides direction for the creating, disabling, reactivating, and changing permissions on user accounts on MarineNet (Booz Allen Hamilton, 2015). Figure 6 contains a flow diagram for the process, and further descriptions of the steps in the Access Control–User Accounts Process appear in Table 1.

Figure 6. Access Control–User Accounts Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 1. The Access Control–User Accounts Process Step-by-Step Description

Step	Activity Details
1	Requestor notifies or concludes that access to the LMS domain is needed for specific task-related activity, and requests access be granted. If the new account is for a standard user, proceed to Step 2. If the new account is for a privileged (i.e., administrative) account, proceed to Step 3.
2	Remedy notifies the IA Analyst of the request. The IA Analyst provides the new account packet that includes forms and required reading material.
3	Remedy notifies the IA Analyst of the request. The IA Analyst provides **privilege** account packet that includes forms and required reading material.
4	The Requestor reviews the provided materials, completes the application/training, and submits the packet to the IA Analyst. If the individual is a new user, proceed to Step 6. If the individual will receive a privilege account, proceed to Step 5.
5	The Requestor provides certification documentation to the IA Analyst.
6	The IA Analyst reviews the completed packet and determines whether to grant the request. If the IA Analyst grants the request, proceed to Step 8, otherwise go to Step 7.
7	The IA Analyst provides a written explanation of the reason for denial of the request. Return to Step 5.
8	O&ML reviews the completed packet and accompanying documentation. If the O&ML denies the request, proceed to Step 9. If the OM&L approves the request for a new user, proceed to Step 10. If the approval is for a privilege user, proceed to Step 11.
9	O&ML closes the Remedy ticket after documenting the denial justification. Return to Step 4.
10	O&ML assigns the account creation to an O&MT member who then creates the account.
11	O&ML assigns the account creation to an O&MT member who then creates the **privilege** account.
12	O&MT assigns the appropriate permissions per the role of the new user as outlined in the Remedy ticket.
13	O&MT prepares and sends the IA Analyst a “welcome packet” for the new account holder.
14	The IA Analyst files the account creation paperwork in the local Share Drive.
15	The IA Analyst loads the request documentation to the Share Drive.
16	The Requestor receives the Information Package from the IA Analyst including the credential information and uses the NOC to access the domain with the login information. The process ends.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

The flow of this process may require alteration since much, if not all, of the IT infrastructure will no longer be under direct local control of the DLNOC. This may particularly effect the creation higher privilege or administrator accounts. The following are the questions arise when reviewing this process:

(1) After migration, who is going to control the creation and modification of user accounts?

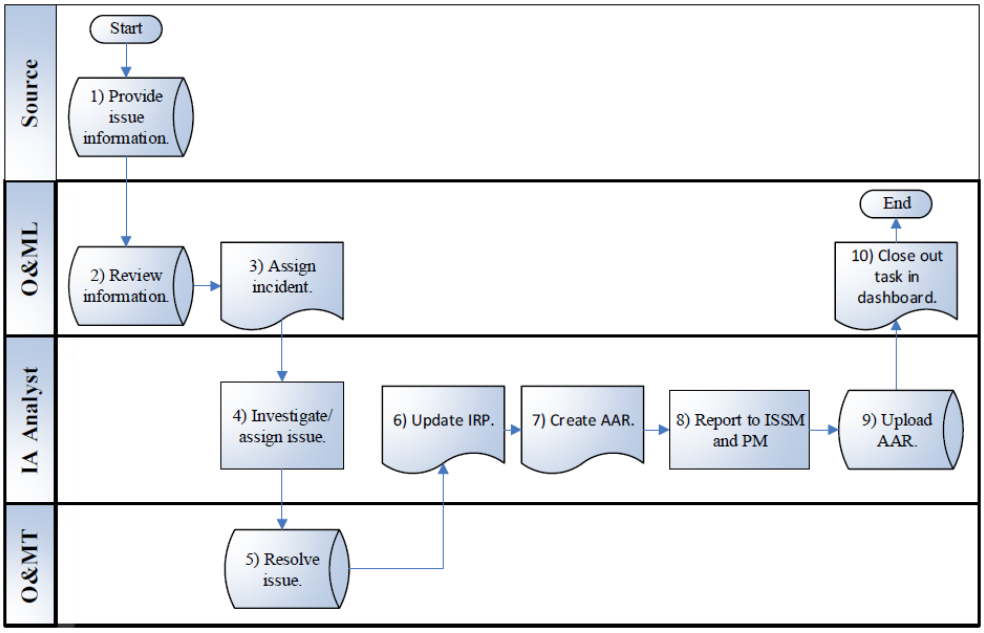
(2) What role, if any, will MCEITS staff have with regards to user account management after the migration?

(3) Will creation of privileged account users require the approval and involvement of MCEITS staff? If so, how will that process work?

b. Incident Reporting and Handling Process

The responsibility for documentation of identified incidents and security threats falls to the to the O&MT. The process begins when a Source discovers a security incident and informs the O&ML by opening a ticket in Remedy. Required outputs of the process include an Incident Response Plan (IRP) and an After Action Report (AAR). Figure 7 provides a graphical representation of the Incident Reporting and Handling Process, while Table 2 presents a step-by-step description.

Figure 7. Incident Reporting and Handling Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 2. The Incident Reporting and Handling Process Step-by-Step Description

Step	Activity Details
1	The Source provides information about an issue by opening a ticket in Remedy.
2	Remedy forwards the issue to the O&ML who reviews the information and documents the issue in the tasking dashboard.
3	The O&ML assigns the ticket to an IA Analyst.
4	The IA Analyst conducts an investigation, creates resolution options, and then assigns the issue to the O&MT to perform necessary corrective actions.
5	Upon completion, the O&MT refers the task back to the IA Analyst.
6	The IA Analyst updates the Incident Response Plan (IRP).
7	The IA Analyst creates an After Action Report (AAR).
8	The IA Analyst sends the AAR to the Information Security System Manager and the Program Manager (PM).
9	The IA Analyst uploads the AAR to the share drive for future reference.
10	The O&ML then closes the ticket in Remedy.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

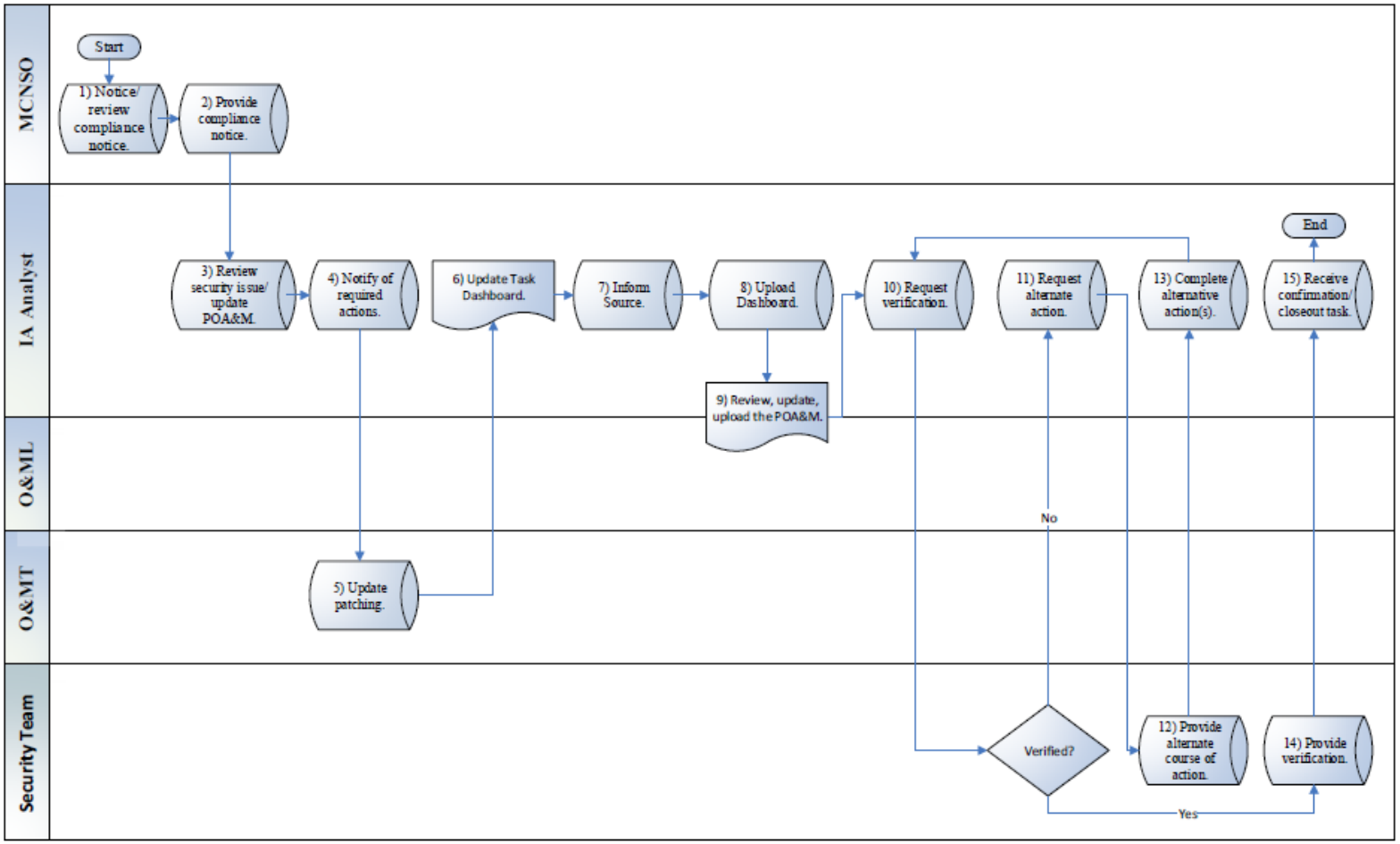
The potential need to alter the process stems from the fact that the infrastructure for MarineNet is no longer under the control of the DLNOC alone. Questions arise regarding which organization creates, submits, submits and receives the plans and reports generated by the current process. Specifically, the research questions for the Incident Reporting and Handling Process are the following:

1. Who will be responsible for incident reporting and handling after the migration to MCEITS?
2. Which organization (CDET or MCEITS) will update the IRP and create the AAR?
3. Where will the responsibilities be divided, if applicable?

c. Compliance Reporting Process

The Compliance Reporting Process provides direction for handling all security notices and reviews. The Marine Corps and Navy Security Officer (MCNSO) maintains awareness on all published security notices and alerts the IA Analyst via email (Booz Allen Hamilton, 2015). Under the current process, the IA Analyst is ultimately responsible for ensuring execution of the process to completion (Booz Allen Hamilton, 2015). Other parties involved in the process are the O&ML, O&MT, and the Security Team. A graphical illustration of the Compliance Reporting Process (Booz Allen Hamilton, 2015) appears in Figure 8, and a more detailed description of the process is in Table 3.

Figure 8. Compliance Reporting Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 3. The Compliance Reporting Process Step-by-Step Description

Step	Activity Details
1	The Marine Corps and Navy Security Officer (MCNSO) notices and reviews the security notice(s).
2	The MCNSO provides the IA Analyst the security notice(s) and opens a Remedy ticket.
3	The IA Analyst reviews vulnerabilities, security changes requested/needed, determines the patches required and steps to address security needs, makes a resource assignment, and documents the POA&M and the ticket.
4	The IA Analyst notifies O&MT of the completed research and required patching.
5	O&MT completes the patching.
6	The IA Analyst updates the Task Dashboard (i.e., a tracking sheet) and closes the ticket.
7	The IA Analyst informs the Source of the resolution.
8	The IA Analyst uploads the Task Dashboard to the Marine Corps Standard Patching and Incident Reporting SharePoint (SIPR SP).
9	O&ML meets with the IA Analyst to prepare and update/upload the POA&M to mitigate future security issues.
10	The IA Analyst requests a Security Team verification. If compliance is verified, proceed to Step 14. Otherwise, proceed to Step 11.
11	The IA Analyst requests an alternative course of action from the Security Team.
12	The Security Team provides an alternate course of action.
13	The IA Analyst completes the alternative action(s). Return to Step 10.
14	The Security Team verifies compliance and provides the IA Analyst verification.
15	The IA Analyst receives approval and instructions to close out the security issue from the Security Team. The process ends.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

The migration to the MCEITS hosting environment raises questions regarding the security compliance responsibilities. The research questions for the Compliance Process are the following:

1. After the migration, who will be responsible for compliance processing and reporting?
2. Which organization will report to and control the implementation of the Security Team's alternative course of action(s)?

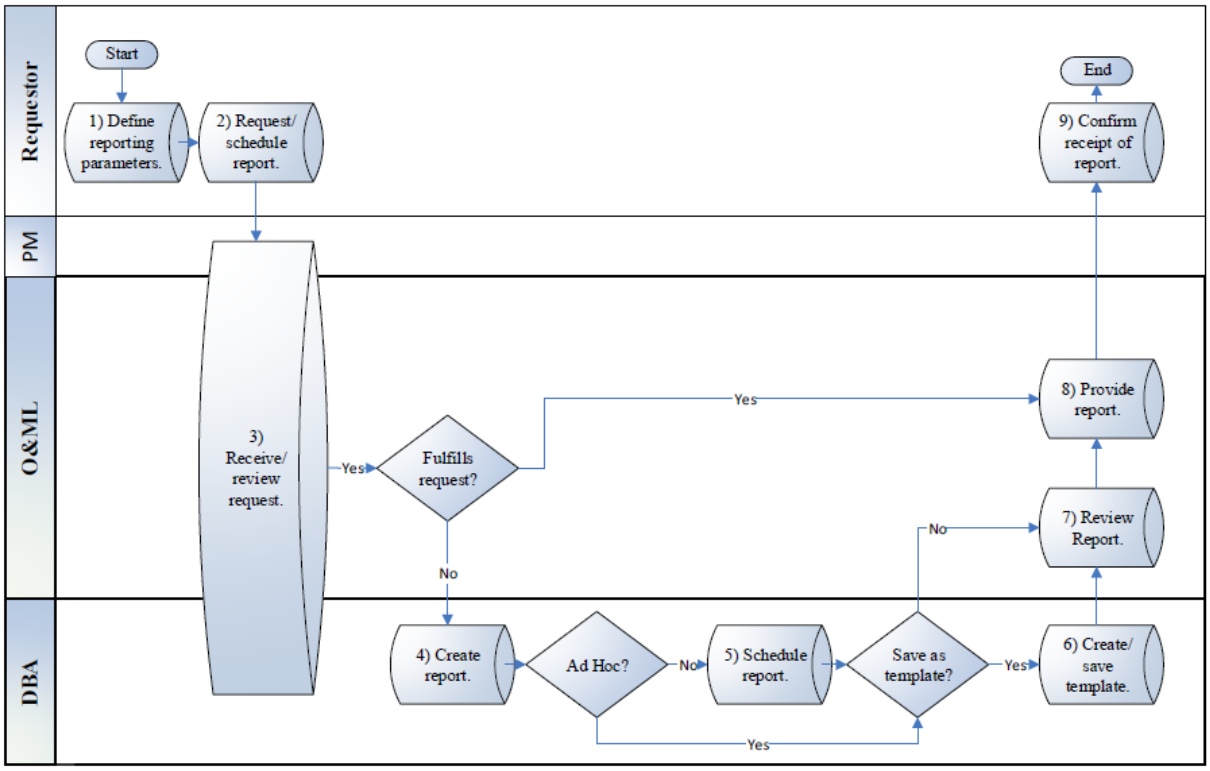
2. Database Administrator Functions

The Database Administrator (DBA) supports the DLNOC with all aspects of database management. The DBA's responsibilities include reporting tasks and database restoration/backup tasks (Booz Allen Hamilton, 2015). This section will include an analysis of the Ad Hoc/Canned Reporting Process, the Database/System Restore Process (Stage), the Database/System Restore Process (Production), and the Monthly Backup Offsite Storage Process.

a. Ad Hoc/Canned Reporting Process

The Ad Hoc/Canned Reporting Process provides guidance on generating reports that are either address unique questions (Ad Hoc) or provide information that will be requested on a routine basis (Canned). A requesting Source initiates the process by contacting the Program Manager (PM), O&ML, or the DBA directly (Booz Allen Hamilton, 2015). The graphical depiction and step-by-step description of the process appears in Figure 9 and Table 4, respectively.

Figure 9. Ad Hoc/Canned Reporting Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 4. The Ad Hoc/Canned Reporting Process Step-by-Step Description

Step	Activity Detail
1	The Requestor defines the specific reporting parameters required for the report.
2	A Requestor contacts the Program Manager (PM), O&ML, or Database Administrator (DBA) and requests a customized report.
3	The O&ML, PM, or DBA receives the request for an ad hoc report. The O&ML and DBA will review the request together and determine whether or not an existing template will fulfill the reporting parameters. If a template exists, proceed to Step 7. Otherwise, proceed to Step 4.
4	The DBA creates the report and determines whether or not to save the report as a template. If the report is to be a "canned" report, proceed to Step 5. If the report is to be an ad hoc report, determine whether the report is to be saved as a template. If it is to be saved as a template, proceed to Step 6. If the "canned" report is not saved as a template, proceed to Step 7.
5	The DBA schedules the new report to generate according to the schedule outlined in the report's parameters.
6	The DBA saves the report as a template.
7	O&ML reviews the customized report. If the report is acceptable, proceed to Step 8. If the report is unacceptable, return to Step 4.
8	O&ML submits the customized report to the Requestor.
9	The Requestor receives the customized report from the O&ML and confirms receipt. The process ends.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

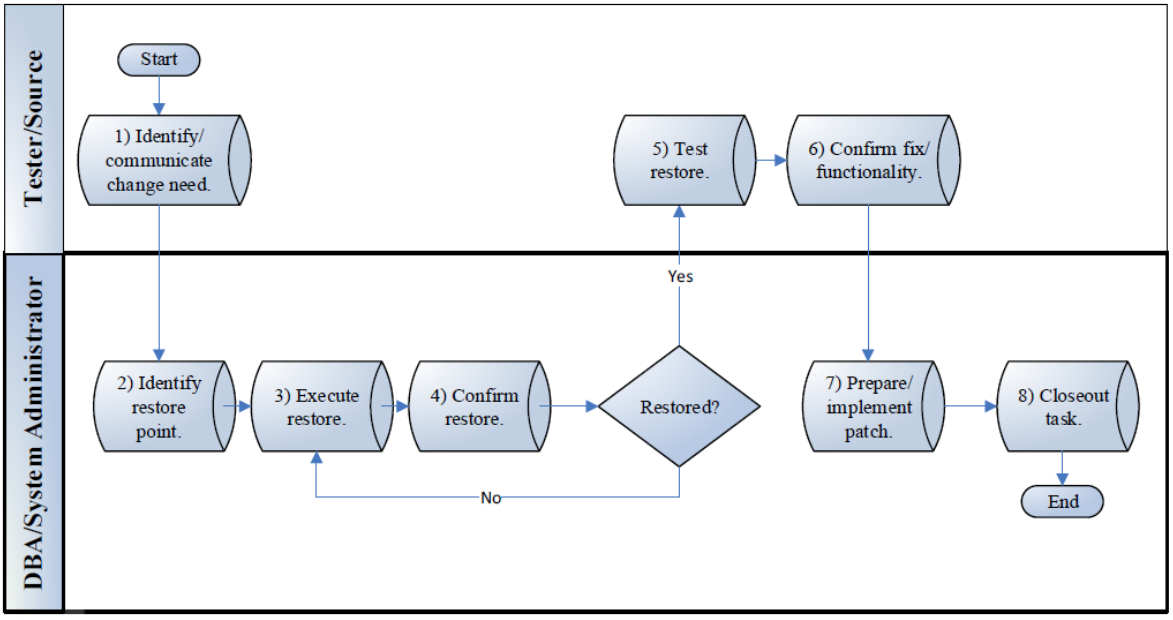
The migration to the MCEITS hosting environment leaves questions regarding how much direct control will the DLNOC maintain. Specifically, the follow questions require answering:

1. Will the DBA continue to work for CDET and the DLNOC, or will DBA duties move to MCEITS?
2. How will the communication flow between the organizations post migration?

b. Database/System Restore (Stage) Process

A Tester/Source or the DBA can initiate the Database/System Restore (Stage)Process upon finding an error or determining the need for a reset within the Stage, or testing, environment (Booz Allen Hamilton, 2015). In the Stage environment, the Database/System Restore Process does not require O&ML approval and is at the discretion of the DBA (Booz Allen Hamilton, 2015). The Database/System Restore (Stage) Process flow chart appears in Figure 10 with a detailed description in Table 5.

Figure 10. Database/System Restore (Stage)



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 5. The Database/System Restore (Stage) Step-by-Step Description

Step	Activity Detail
1	The Tester or other Source identifies the need for a change in the database or system. If a database change is required, the Tester informs the DBA. If a system change is required, the system administrator is informed. When the Tester identifies a need, he/she opens a ticket in Remedy.
2	The DBA or System Administrator identifies the restore point.
3	The DBA or System Administrator executes the restore.
4	The DBA or System Administrator confirms the restore took place in Stage. If the database or system was not restored, return to Step 3. If the database or system was restored, proceed to Step 5.
5	The Tester determines (i.e., tests) whether or not the data was restored in Stage.
6	The Tester confirms that the "fix" in the database/system restored all functionality in Stage.
7	The DBA or System Administrator prepares and implements a patch for the system.
8	The DBA or System Administrator closes out the task in the dashboard, and closes the ticket.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

The migration raises concern about CDET and the DLNOC's future access to a Stage/testing environment equivalent in MCEITS. The questions regarding the Database/System Restore (Stage) Process are:

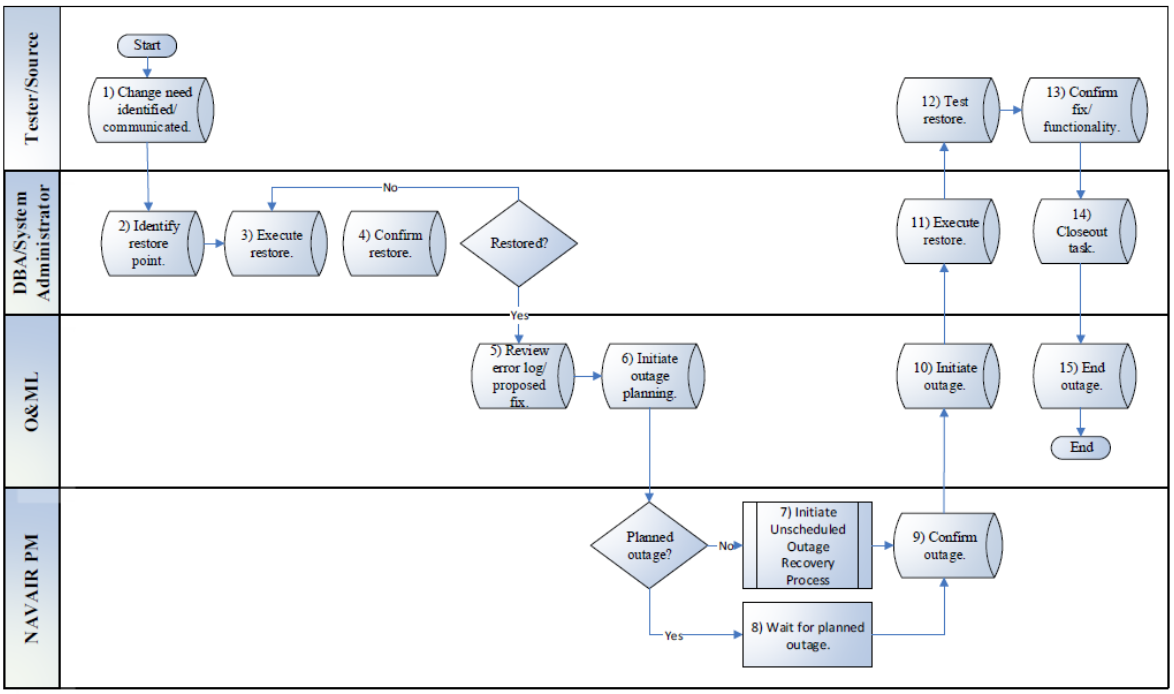
1. Will DLNOC Testers and the DBA have direct access to the MCEITS Zone A testing environment, or will access require coordination with MCEITS personnel?
2. Once a tested solution is developed, what coordination with MCEITS personnel is necessary to implement the solution in the Production environment?

c. Database/System Restore (Production) Process

The Database/System Restore (Production) Process is similar to the previously discussed Stage Process except it involves the Production (or Active) working environment. Involvement of the Production environment adds complexity to the process

that requires O&ML and NAVAIR PM approval along with coordination with the DLNOC Help Desk (Booz Allen Hamilton, 2015). When dealing with the Production environment, the parties involved must determine if the database/system restore can take place during a scheduled outage or if it requires an emergency outage and resolution (Booz Allen Hamilton, 2015). Restoration after an outage requires the completion of testing prior to bringing the Learning Management System back online (Booz Allen Hamilton, 2015). A graphical depiction of the Database/System Restore (Production) Process appears in Figure 11, and Table 6 contains a detailed description.

Figure 11. Database/System Restore Process (Production)



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 6. The Database/System Restore Process (Production) Step-By-Step Description

Step	Activity Details
1	The Tester identifies the need for a change in either the database or system and notifies the DBA if a database change is required or the System Analyst if a system change is required.
2	The DBA or System Analyst receives notification of the database/system and identifies the restore point.
3	The DBA or System Analyst executes the restore in Stage.
4	The DBA or System Analyst confirms the restore completed. If the restore did not complete, return to Step 3. If the restore did complete, proceed to Step 5.
5	O&ML reviews the error log and the proposed fix.
6	O&ML initiates the outage planning. If the fix can wait until the next planned outage, proceed to Step 7. If the fix cannot wait until the next planned outage, proceed to Step 8.
7	O&ML initiates the Unscheduled Outage Recover Process.
8	The NAVAIR PNM waits until the next scheduled outage for the affected system.
9	The NAVAIR PM confirms the outage schedule with CDET.
10	O&ML initiates outage at the schedule time/date.
11	The DBA or O&MT System Analyst executes the restore in Production.
12	The Tester assesses the restore in Production.
13	The Tester confirms the fix and functionality in Production and notifies the DBA or the System Administrator.
14	The DBA or the System Administrator closes out the task in the Task Dashboard and the ticket in Remedy.
15	O&ML ends the outage. The process ends.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

The migration to MCEITS creates the possibility of adding even more complexity to an already complex process. As previously discussed, questions exist regarding the direct access of CDET and DLNOC personnel to the database and a testing environment. Additional questions for the research involve the following:

1. What control with the DBA or the System Administrator have regarding unscheduled outages?
2. Who will perform the required testing before bringing the LMS back online?
3. What involvement from MCEITS personnel be required to complete this process once the migration is complete?

d. Monthly Backup Offsite Process

The Monthly Backup Offsite Process ensures that a rollback ready version of the LMS is available in the event of a catastrophic failure (Booz Allen Hamilton, 2015). In addition, the data associated with the database is backed up for the previous 90 days (Booz Allen Hamilton, 2015). The process involves the use of tape drives that stored offsite and are routinely recycled (Booz Allen Hamilton, 2105). Unfortunately, a diagram of the process was unavailable, but Table 7 provides a step-by-step description

Table 7. Monthly Backup Offsite Process Step-by-Step Description

Step	Activity Details
1	O&MT initiates the monthly backup of the LMS.
2	O&MT retrieves the monthly backup tapes.
3	The DLNOC Librarian opens the Caddie-Request-Shipping.
4	The NAVAIR PM reviews the file log, data un, shipping information, and other pertinent information. The NAVAIR PM determines whether or not to authorize the monthly offsite storage backup. If the information is restored, proceed to Step 5. Otherwise, return to Step 3.
5	The DLNOC Librarian confirms the shipping details and prints/adheres shipping label.
6	The DLNOC Librarian ships the monthly backup tapes to the offsite storage site.
7	The Program Manager for Training Systems (PM TRASYS) receives the monthly backup tapes and archives them.
8	The PM TRASYS ships the archived tapes to the DLNOC every 90 days.
9	O&MT receives the archived tapes.
10	O&MT recycles the archived tapes, ending the process.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Given that MCEITS may have already established backup procedures, the process may become unnecessary once the migration is complete. Specifically, the questions covered in the research will include:

1. Will DLNOC personnel need to participate in the Monthly Backup Process, or will monthly backups be part of MCEITS internal processes?
2. Will CDET or the DLNOC have any say in the way database/system backups are conducted?

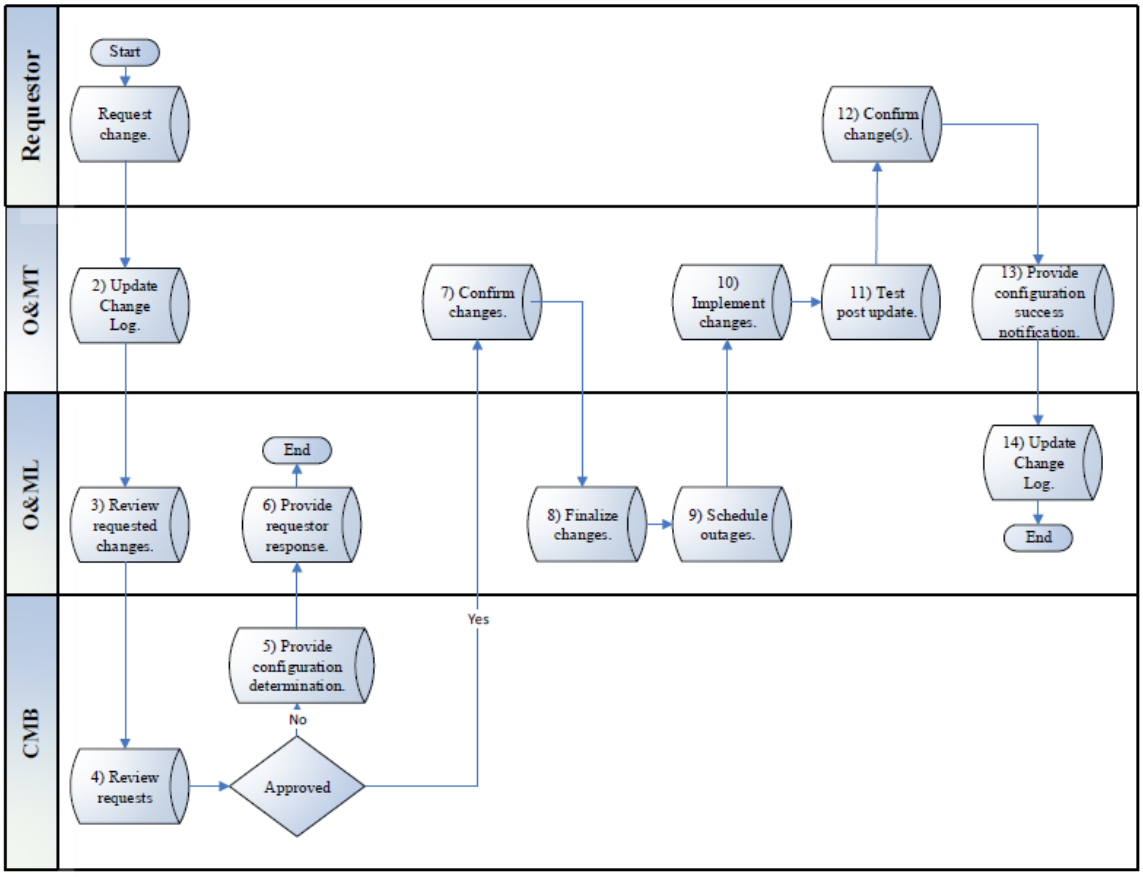
3. Hosting and Network

The DLNOC processes under the Hosting and Network functional area face the potential for great change during the MCEITS migration. Under the current system setup, the DLNOC Hosting and Network Team maintains the physical state of the DLNOC servers and their connectivity (Booz Allen Hamilton, 2015). Furthermore, the Hosting and Network team manages configuration, patches, and outage recovery for the system (Booz Allen Hamilton, 2015). With the migration of the DLNOC infrastructure to MCEITS, the duties of the Hosting and Network team will receive significant restructuring. The processes reviewed in this section include the Change Request Process, Patch Management Process, the LMS Release Management Process, Outage Scheduling Process, and Unscheduled Outage Recovery Process.

a. Change Request Process

The Change Request Process is a process that addresses the physical server environment at the DLNOC. A change request involves a change to the configuration of the servers that involves work by the O&MT, reviews by the O&ML, and requires the approval of the Change Management Board (CMB). Figure 12 outlines and Table 8 provides a step-by-step description of the current process.

Figure 12. Change Request Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 8. The Change Request Process Step-by-Step Description

Step	Activity Detail
1	The Requestor identifies the need for a configuration change and requests it.
2	O&MT receives the request and updates the DLNOC Change Log.
3	O&ML facilitates a meeting with O&MT to review each requested configuration change.
4	The Configuration Management Board (CMB) reviews each configuration change request and determines whether or not to honor the request. If the request is not honored, proceed to Step 5. If the request is honored, proceed to Step 7.
5	The CMB informs the O&ML of their decisions regarding the configuration request.
6	O&ML notifies the requestor of the denied configuration request. The process ends.
7	O&ML enters "CONFIRMED" in the change log to confirm the final configuration changes.
8	O&ML reviews the final configuration change(s) and determines the time required to implement the change(s).
9	O&ML creates schedules an outage that will be used to implement and notifies O&MT.
10	O&MT makes the specified changes.
11	O&MT tests the update and notifies the Requestor when the testing is completed. Note: This step is referred to as a "high level smoke test."
12	Requestor checks the system changes to verify functionality/capability and reports findings to O&MT.
13	O&MT informs O&ML with confirmation of successful configuration change.
14	O&ML updates the Change Log and closes the process.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

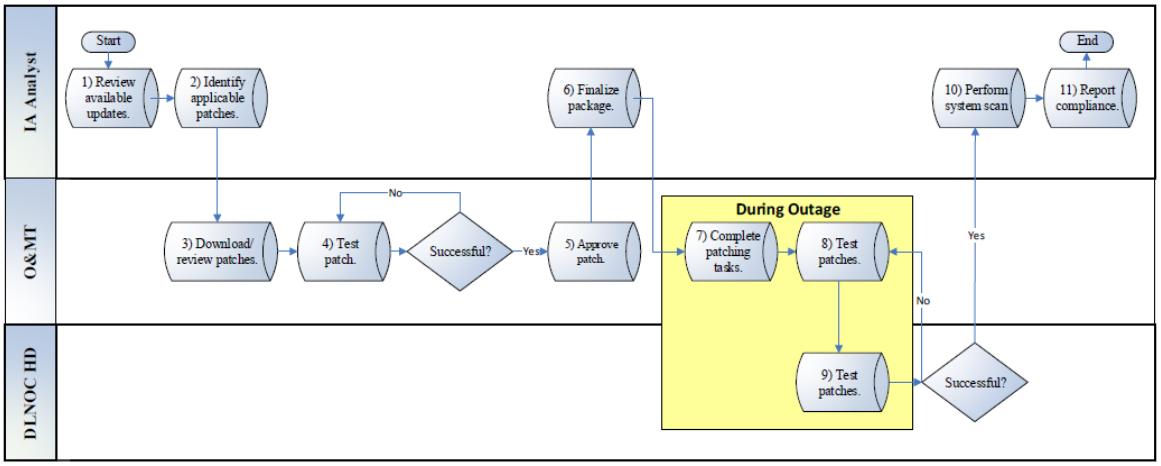
The migration to MCEITS would provide that most, if not all, of the physical infrastructure would move to virtual servers within the Kansas City datacenter. The current Change Request Process will require radical restructuring. Questions for the research include:

1. How will change requests be handled once the migration to MCEITS's virtual servers is complete?
2. Will MCEITS allow for change requests, and if so, how much direct control will CDET and the DLNOC maintain?

b. Patch Management Process

The Patch Management Process is another process that faces vast restructuring under the MCEITS migration. The current Patch Management Process provides guidance for applying security and other patches for the LMS software and server operating system software (Booz Allen Hamilton, 2015). Currently, the responsibility of managing patches falls to the IA Analyst and the process involves the O&MT and the DLNOC Help Desk. The current process appears in Figure 13, and a detailed description is in Table 9.

Figure 13. Patch Management Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 9. The Patch Management Process Step-by-Step Description

Step	Activity Detail
1	The IA Analyst reviews the available Microsoft (MS) updates.
2	The IA Analyst identifies the applicable patches.
3	O&MT downloads, reviews, and packages the applicable patches.
4	O&MT tests the patch in Stage. If the test is successful, proceed to Step 5. If the test is not successful, return to Step 4.
5	O&MT approves the patch to be installed during the IA outage.
6	The IA Analyst finalizes the patch package to be implemented during the IA outage.
7	O&MT completes all of the patch activities.
8	O&MT tests the patch in Production and notifies the DLNOC Help Desk (HD) when their test is completed. Note: The testing process is documented and placed on the Shared Drive. This test is also referred to as a "smoke test." Often a ticket is opened for this step in Remedy, and it is assigned to the O&ML. When a second level of testing is completed, the O&ML re-assigns the ticket to the DLNOC HD. Testing results are documented and this step is completed during an IA outage.
9	DLNOC HD repeats the patch testing and documents the testing results in the Remedy ticket. If the testing is not successful, repeat Step 8. If the testing is successful, update/close the ticket and proceed to Step 10. This step is completed during an IA outage.
10	The DLNOC IA System Analyst performs a full system scan. Note: This scan process is fully documented and available of the Shared Drive.
11	DLNOC IA System Analyst reports the compliance based upon the scan results to the original initiator. The process ends.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Similar to the Change Request Process, the current Patch Management Process may become obsolete once the migration to MCEITS's virtual servers is complete. The following questions require addressing in order develop a new Patch Management Process:

1. After migration, will CDET and the DLNOC needs to have a process for addressing patches for the server operating systems?
2. Will MCEITS apply all server operating system patches?

3. Will the DLNOC still be responsible for applying LMS software patches?

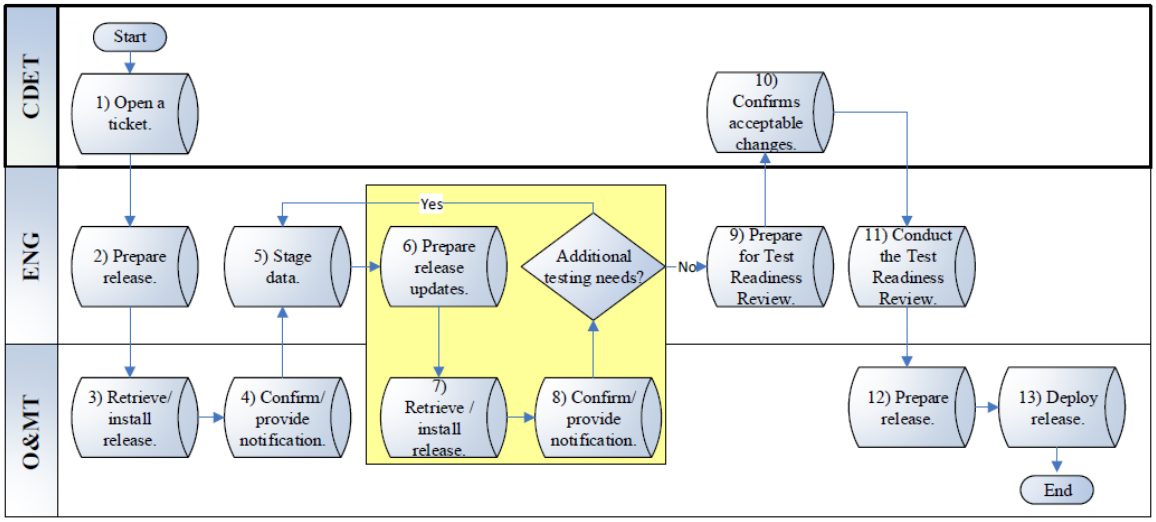
4. What coordination will need to occur between MCEITS and CDET/DLNOC to apply security, LMS, and operating system patches?

5. Who will be responsible for patch testing?

c. LMS Release Management Process

The purpose of the LMS Release Management Process is to provide guidance for upload and application of LMS release updates developed by the DLNOC Engineering Team (ENG) (Booz Allen Hamilton, 2015). These updates normally receive testing in the Stage environment prior to any upload to the Production environment (Booz Allen Hamilton, 2015). Figure 14 contains a graphical illustration of the current process, which involves CDET, the ENG, and the O&MT. Table 10 provides a Step-by-Step Description

Figure 14. LMS Release Management Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 10. The LMS Release Management Process Step-by-Step Description

Step	Activity Detail
1	CDET opens a ticket to initiate the LMS release.
2	DLNOC Engineering Team (ENG) prepares a development release in Production.
3	O&MT retrieves the release and installs it in Stage 2.
4	O&MT confirms the release and provides an installation notification.
5	ENG stages the data.
6	ENG prepares additional release updates.
7	Retrieve/install release in Stage 2.
8	O&MT confirms the release and provides an installation notification.
9	ENG prepares for the Test Readiness Review.
10	CDET confirms that the changes are acceptable.
11	ENG conducts the Test Readiness Review.
12	O&MT prepares the release for Production.
13	O&MT deploys the release to Production, Stage 1, Stage 2, and Stage 3 ending the process.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

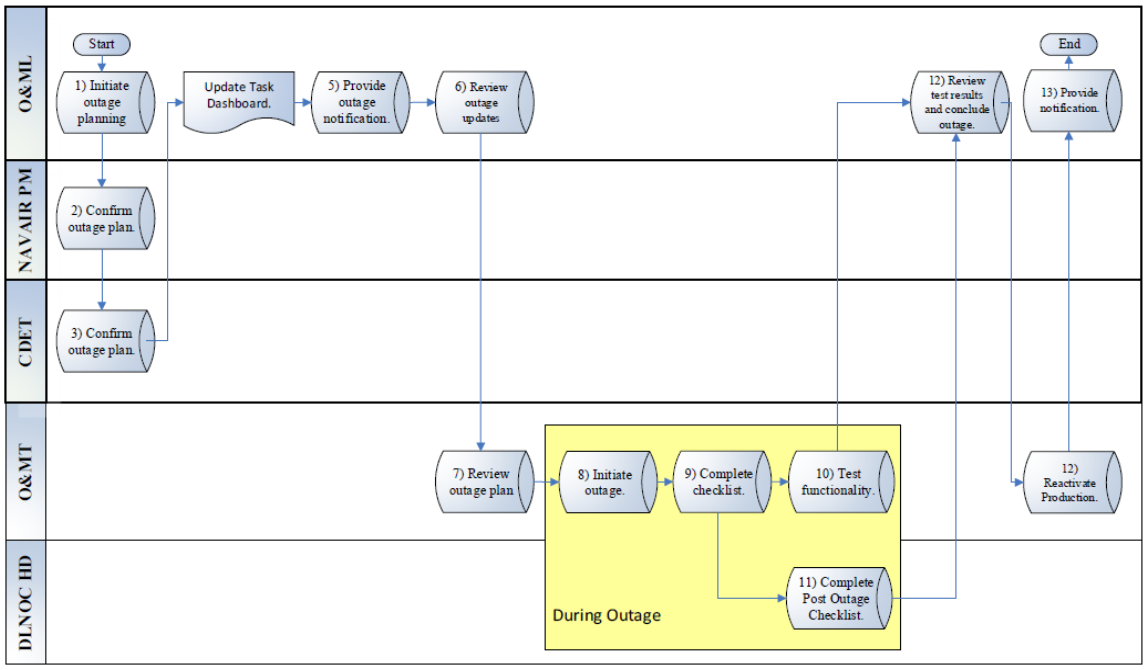
Questions regarding changes to the LMS Management Process are similar to those presented for previous processes. Those questions include:

1. What kind of testing environment will MCEITS provide for the development and testing of LMS updates?
2. What roles will MCEITS personnel play in the update application process?
3. How much direct control will DLNOC personnel have on the update application process?

d. Outage Scheduling Process

Under the current process, the O&ML holds responsibility for scheduling, executing, and recovering from an outage due to the application of a software patch, release, or update (Booz Allen Hamilton, 2014). Figure 15 illustrates the current process, and Table 11 provides a detailed description.

Figure 15. Outage Scheduling Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 11. The Outage Scheduling Process Step-by-Step Description

Step	Activity Detail
1	O&ML plans an outage and informs the NAVAIR PM of the plan.
2	The NAVAIR PM confirms the outage plan and notifies CDET.
3	CDET confirms the outage plan and notifies the O&ML.
4	O&ML assigns a resource to the outage and updates the Task Dashboard with the resource information.
5	O&ML notifies the LMS stakeholders of the outage events.
6	O&ML reviews the outage updates.
7	O&MT the outage plan.
8	O&MT initiates the outage per the outage schedule.
9	O&MT completes the activities that are outlined in the Outage Checklist.
10	O&MT tests the affected system's/LMS's functionality and confirms.
11	The DLNOC Help Desk completes the Post Outage Checklist (POC) and notifies the DLNOC O&M.
12	O&MT reactivates LMS in Production and concludes the outage.
13	O&ML notifies stakeholders that the outage has ended and the next scheduled outage via e-mail. The process ends.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

The post migration Outage Scheduling Process will need to define who gets to initiate and control outages in the system. Specifically, the follow questions arise:

1. Who will control the schedule for the outages?

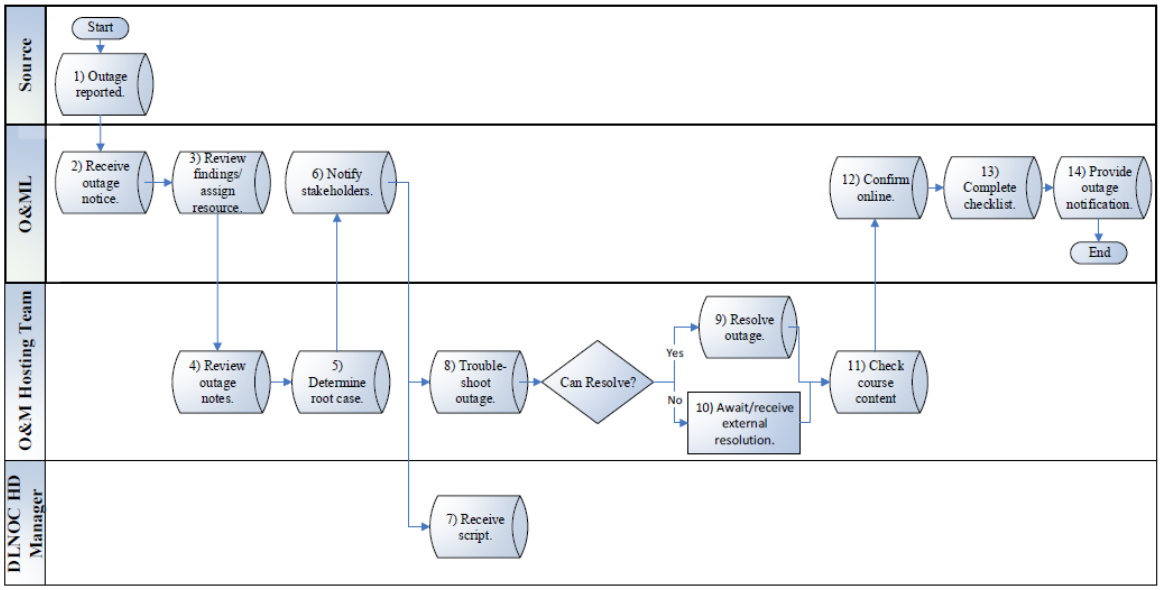
2. What involvement will MCEITS have in the process?

e. Unscheduled Outage Recovery Process

The Unscheduled Outage Recovery Process provides guidance for emergency and unplanned outages. During this process, patches and updates require testing in parallel

between the Hosting Team and the DLNOC Help Desk to quickly restore system functionality (Booz Allen Hamilton, 2015). An unscheduled outage involves the DLNOC Help Desk because Help Desk staff must be ready to answer inquiries from end users regarding the system status (Booz Allen Hamilton, 2015). The O&ML is responsible for providing the Help Desk with what informtions is to be released to end users (Booz Allen Hamilton, 2015). Figure 16 depicts the work flow for the process, and Table 12 provides the detailed description.

Figure 16. Unscheduled Outage Recovery Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 12. The Unscheduled Outage Recovery Process

Step	Activity Detail
1	A Source notifies the O&ML of a possible outage via an automated report or through and increase in Help Desk tickets.
2	O&ML receives the outage notification.
3	O&ML reviews outage findings and assigns a resource to the outage.
4	O&M Hosting Team of the affected system review the outage notes.
5	O&M Hosting Team determines the outage's root cause.
6	O&ML notifies the affected system's stakeholders to the root cause.
7	DLNOC Help Desk Manager receives the script to share with callers regarding an unplanned outage.
8	O&M Hosting Team troubleshoots outage or awaits external resolution. If the incident can be resolved, proceed to Step 10. If the incident cannot be resolved, proceed to Step 9.
9	O&M Hosting Team resolves the outage.
10	O&M Hosting Team receives resolution from external sources.
11	O&M Hosting Team checks the LMS course content.
12	O&ML confirms that the LMS is online and available to use.
13	O&ML completes the Scheduled Outage Checklist.
14	O&ML provides stakeholders an outage status notification. The process ends.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

The Unscheduled Outage Process will require restructuring after the migration since MCEITS personnel will need to participate in the determining the cause of the outage. The research questions for this process are the following:

1. Who will take charge during an unscheduled outage?
2. Who will be responsible for providing the DLNOC Help Desk with guidance during the outage?

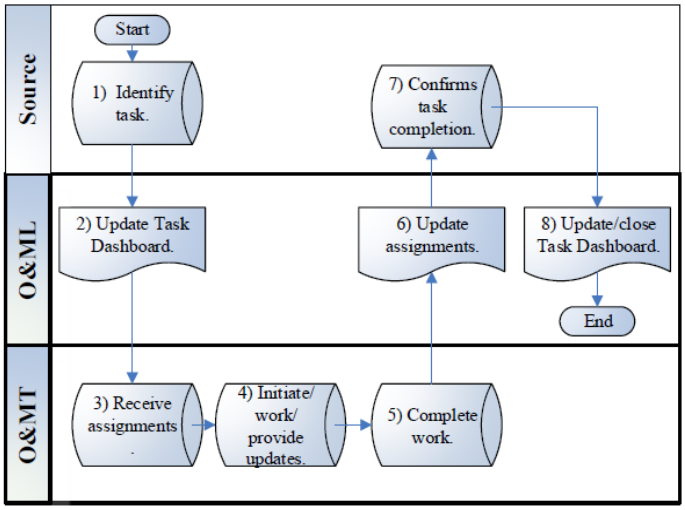
4. Administration

Currently, the O&ML is responsible for administrative functions for the DLNOC to include the Tasking Process and the Procurement Process (Booz Allen Hamilton, 2015).

a. Tasking Process

The O&ML collaborates with the NAVAIR PM to track project tasks and updates the task dashboard with task prioritization and completion dates (Booz Allen Hamilton, 2015). A graphical illustration of the Tasking Process appears in Figure 17, and the step-by-step description is in Table 13.

Figure 17. Tasking Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 13. The Tasking Process Step-by-Step Description

Step	Activity Detail
1	A Source identifies a task for the O&MT and informs the O&ML.
2	O&ML adds the task information including tasks and resource assignments to the Task Dashboard that is maintained on the Shared Drive.
3	O&MT receives the tasks and task assignments in person, e-mail and/or Remedy.
4	O&MT begins the work per the assignment. All information regarding the status of the task is updated in the ticket details.
5	O&MT completes the task per the assignment and closes the corresponding ticket.
6	O&ML updates assignments to load balance the workload.
7	Source confirms to the O&MT or O&ML that the task has been completed.
8	The O&ML closes the tasking in the Task Dashboard. The process ends.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

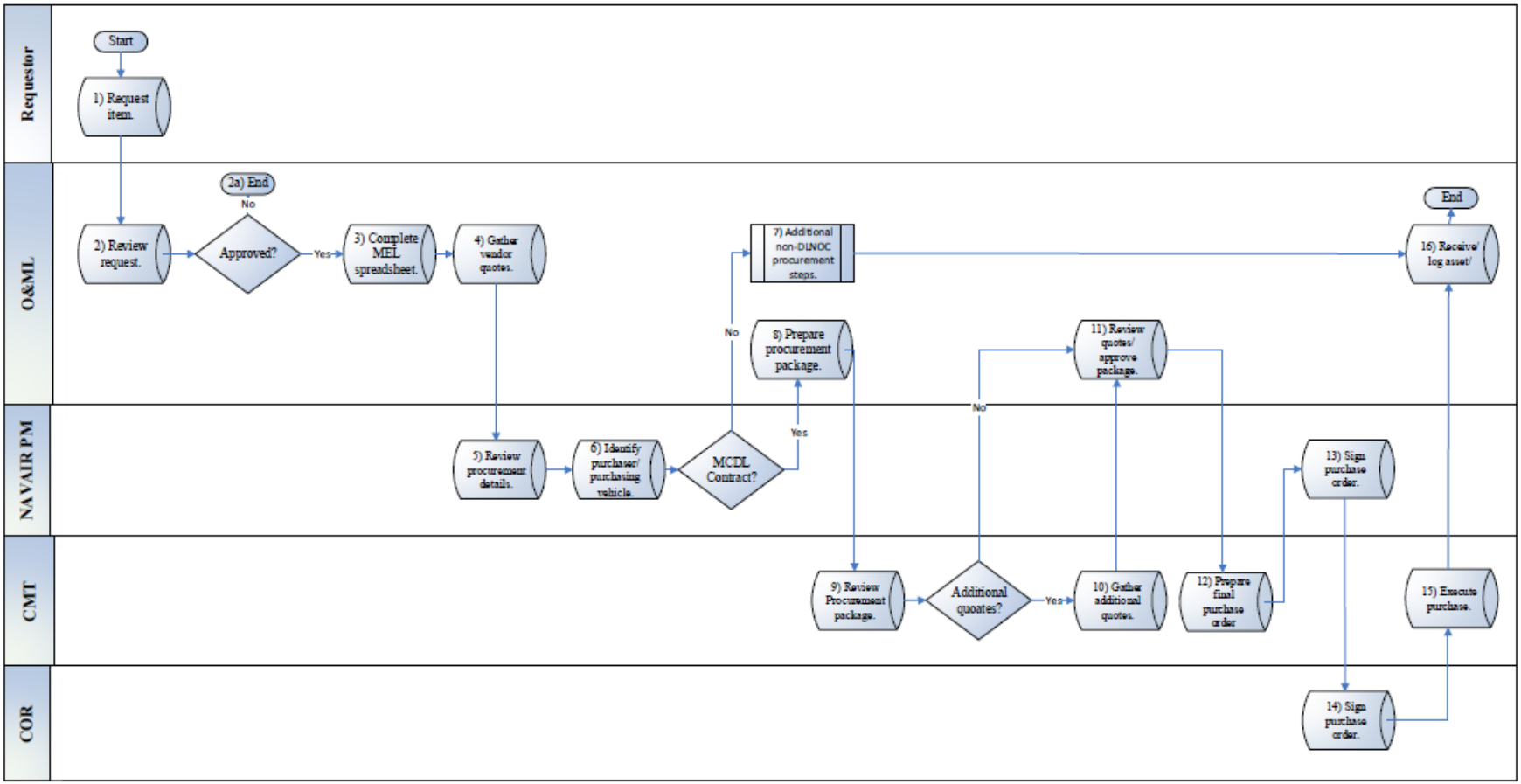
The post-migration Tasking Process will need to address the following questions:

1. Will the O&ML be able to assign tasks to MCEITS personnel, if required?
2. How will communication between CDET, DLNOC, and MCEITS personnel be conducted for completing tasks?

b. Procurement Process

The Procurement Process describes the steps for acquiring hardware and software for the DLNOC. Under the current process, the O&ML reviews and verifies procurement requests and discusses them with the NAVAIR PM (Booz Allen Hamilton, 2015). If the O&ML and NAVAIR PM approve a procurement request, the O&ML will contact the Contract Management Team (CMT) who will then obtain vendor quotes (Booz Allen Hamilton, 2015). Once the CMT prepares the final purchase order, the CMT forwards it to the O&MT, NAVAIR PM, and the Contract Officer Representative (COR) for review and signing (Booz Allen Hamilton, 2015). Once the final purchase order receives all signatures, the CMT executes the purchase order (Booz Allen Hamilton, 2015). Figure 18 provides a graphical illustration, and Table 14 contains a detailed step-by-step description of the current Procurement Process.

Figure 18. Procurement Process



Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

Table 14. The Procurement Process Step-by-Step Description

Step	Activity Detail
1	Requestor asks for a specific asset that requires procurement and includes the justification for the asset.
2	The O&ML reviews the request and justification. If the request is approved, proceed to Step 3. If O&ML denies the request, O&ML provides the reason for the denial and process ends.
3	O&ML completes the MEL spreadsheet, which is available on the Shared Drive.
4	O&ML requests and collates pricing quotes from a minimum of 3 vendors.
5	The NAVAIR PM will review vendor quotes as prepared by the O&ML including cost estimate, delivery timeline, and support (if applicable) prior to selecting a funding vehicle.
6	NAVAIR PM identifies the purchaser and the purchasing vehicle to be used. If the contracting vehicle to be used is the Marine Corps Distance Learning (MCDL) contract, proceed to Step 8. If the contracting vehicle to be used is not the MCDL contract, determine if additional quotes are required. If additional quotes are needed, proceed to Step 10. If additional quotes are not needed, proceed to Step 11.
7	DLNOC staff has no further actions to take until the asset is received.
8	O&ML prepares the procurement package.
9	O&ML reviews the quotes and the procurement package and grants the package approval. If additional quotes are required, proceed to Step 10. If no additional quotes are required, proceed to Step 11.
10	Contract Management Team (CMT) obtains additional quotes per the O&ML's direction.
11	O&ML will review the draft procurement package including any additional vendor quotes received by the Material Team. This step insures that item(s) to be procured will meet the final need or intended need of the initial requestor.
12	CMT prepares the final purchase order.
13	NAVIAR PM reviews and signs the final purchase order. NAVAIR PM then provides the signed purchase order to the Contract Officer Representative (COR).
14	COR reviews and signs the final purchase order that has been signed by the NAVAIR PM.
15	CMT confirms the approval of the asset and places the purchase.
16	O&ML receives the new asset and logs the asset. The process ends.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

The Procurement Process will face major alteration since the physical hardware infrastructure will be replaced by virtual servers in the MCEITS hosting environment. Requests for additional hardware will require MCEITS involvement in the process. The future Procurement Process will require the following questions to be addressed:

1. How will the O&ML request additional computing resources from MCEITS?
2. How will the O&ML procure software after the migration? Will the O&ML need to procure software through MCEITS?
3. What will be the role of the MCEITS personnel in the procurement process?

E. MOVING FORWARD

The preceding examination of the DLNOC's SOPs reveals that each process faces the possibility of alteration after the migration to MCEITS. Prior to commencing the migration, CDET and MCEITS personnel should address each of the raised questions to ensure a smooth transition with minimal service disruptions. These questions will provide the basis for the research and analysis presented in the next chapter.

IV. RESEARCH AND ANALYSIS

This chapter begins with an overview of interviews conducted with Marine Corps Enterprise Information Technology Services (MCEITS) personnel to understand the organization's internal procedures and processes for interacting with its customers. The intent of the interviews was to address questions that could not be directly answered through MCEITS documentation alone. Specifically, the interviews focused on how the MCEITS migration will affect the Distance Learning Network Operation Center's (DLNOC) current standard operating procedures in order to answer the questions presented in Chapter III.

The second part of this chapter will present proposed changes to the DLNOC's standard operating procedures. A review of each proposed "to-be" procedure will include justification for the changes by applying information learned from the interviews. Each procedure will have a diagram representing the new process flow.

A. DOCUMENTATION REVIEW AND INTERVIEWS

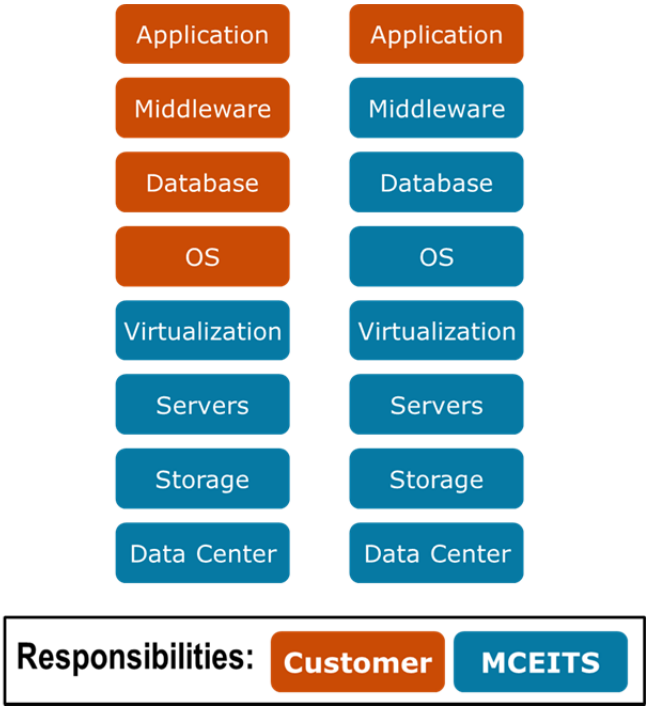
In addition to reviewing MCEITS documentation, the research included interviews with MCEITS personnel. The interviewed personnel were Mr. Mark Johnson, the MCEITS Services Integrated Product Team (IPT) Lead and Maj. Seth Gibson, USMC (Ret.), formerly the Assistant to the MCEITS IPT Lead. The interviews with Mr. Johnson took place via telephone on November 20, 2015, and February 11, 2016. The interview with Maj. Gibson took place in person on February 12, 2016. The questions asked during the interviews focused on three areas of concern—funding, structure, and operations and management.

MCEITS is a program of record whose mission is to provide enterprise IT hosting services to the "Marine Corps decision makers, application owners, information managers, and network user" (HQMC C4, 2012, ¶ 1). MCEITS has its own dedicated funding that the Marine Corps sets at the level required to support Marine Corps programs (M. Johnson, telephone interview, November 20, 2015). Commands that become MCEITS customers do not "pay" for services directly via lines of accounting

(LOAs) or job order numbers (JONs). To date, MCEITS has not had any funding complaints from its customers since their respective migrations (M. Johnson, telephone interview, November 20, 2015).

As mentioned earlier, MCEITS offers two service models, Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Figure 19 shows the division of responsibilities between MCEITS and its customers for purely IaaS service (left column) and purely PaaS service (right column).

Figure 19. MCEITS Service Offerings



Source: Colangelo, D. (2015). Marine Corps enterprise information services (MCEITS) information technology (IT) standards guide version 2.0. Quantico, VA: Marine Corps Systems Command.

During the preparation and migration planning phases, the College of Distance Education and Training (CDET) and MCEITS will negotiate the specifics of the hosting options to be included in the service level agreement (SLA) (Schaefer, 2014). The following assumptions regarding the division of responsibilities are the basis for this analysis:

1. MCEITS will provide the data center, storage, servers, virtualization, server operating systems (OS), the database management system (DBMS), and some standard middleware.
2. CDET will be responsible for its applications, including the database applications, and any middleware that is specific to CDET's applications.

As previously stated, MCEITS will provide CDET's DLNOC personnel with a virtual private network (VPN), web access, server access, system administrator rights, database administrator (DBA) rights and application administrator rights (Colangelo, 2015). Under the PaaS model, MCEITS will maintain responsibility for licensing, patching, and updating the infrastructure software, such as, the server operating systems, database management systems, VPN software, and MCEITS provided middleware (Colangelo, 2015; M. Johnson, telephone interview, November 20, 2015). Therefore, adoption of the PaaS model will be the basis of this analysis.

After the migration, MCEITS will provide the CDET DLNOC with two hosting environments—Zone A and Production (M. Johnson, telephone interview, November 20, 2015). The purpose of the Zone A environment is to provide for final stage testing for patches, updates, and new software (Colangelo, 2015; M. Johnson, telephone interview, November 20, 2015). Zone A is the functional equivalent to the DLNOC's current Stage environment. The Production environment is the real-time, active network for use by CDET's customers (M. Johnson, telephone interview, November 20, 2015). Zone A will be an exact copy of the Production (live and active) environment (M. Johnson, telephone interview, November 20, 2015). When applying OS or DBMS patches or updates, MCEITS's standard procedure is to apply the patch or update in the Zone A environment and notify the customer (M. Johnson, telephone interview, February 11, 2016; S. Gibson, personal interview, February 12, 2016). If neither MCEITS nor DLNOC personnel discover any negative impacts of the software change in the Zone A environment within one week, MCEITS personnel will then apply the patch to the Production environment (M. Johnson, telephone interview, February 11, 2016; S. Gibson, personal interview, February 12, 2016).

Mark Johnson (telephone interview, February 11, 2016) stated that all MCEITS customers maintain Development environments. The Development environment is a smaller-scale, laboratory version of the Zone A and Production environments that the customer retains locally for creating new software, patches, and updates (M. Johnson, telephone interview, February 11, 2016). The DLNOC will need to maintain its Development environment because MCEITS cannot currently support software development (M. Johnson, telephone interview, February 11, 2016). The key to successfully using the Development environment after the migration is to ensure that it stays synchronized with the Zone A and Production environments (S. Gibson, personal interview, February 12, 2016). Staying synchronized means that the Development environment must run the same versions of OS, DBMS, and application software including patches and updates. This analysis will include the assumption that CDET will continue to maintain a Development environment after the migration.

B. DISTANCE LEARNING NETWORK OPERATIONS CENTER POST MIGRATION PROCESS MODIFICATIONS (TO-BE)

Using the assumptions presented in the previous section, the following sections will present the proposed modifications to the DLNOC's standard operating procedures. The proposed changes will affect the four functional areas (Security, Database, Hosting and Network, and Administration). Each proposed process will have a process flow diagram and a step-by-step description similar to the original process. However, changes to the original diagram or description will appear in orange and have labels that start with an "M" followed by a sequentially assigned number. Descriptions for any step that is modified from the original process will begin with "[Modified Step]." Descriptions for steps that are completely new additions to the original process will begin with "[New Step]."

1. Security

Changes to security processes are dependent on the affected system and which organization maintains the responsibility for the system. Interactions with the operating systems, DBMS, and infrastructure will require MCEITS involvement in the process. As

the application owner, CDET would ultimately be responsible security at the application level. The following proposed Access Control–User Accounts Process, Incident Reporting and Handling Process, and Compliance Reporting Process attempt to address this division of responsibilities after the migration.

a. Access Control–User Accounts Process

The Access Control–User Accounts Process flow will require modifications for dealing with privilege accounts. Privileged accounts are accounts that have system administration or DBA permissions. Holder or privileged accounts will have the ability to access and manipulate the Production and Zone A environments via VPN. Creating privilege accounts will require submitting customer support requests to MCEITS customer support. Figure 20 contains the proposed diagram, and Table 15 provides the step-by-step description.

Figure 20. Proposed Access Control–User Accounts Process

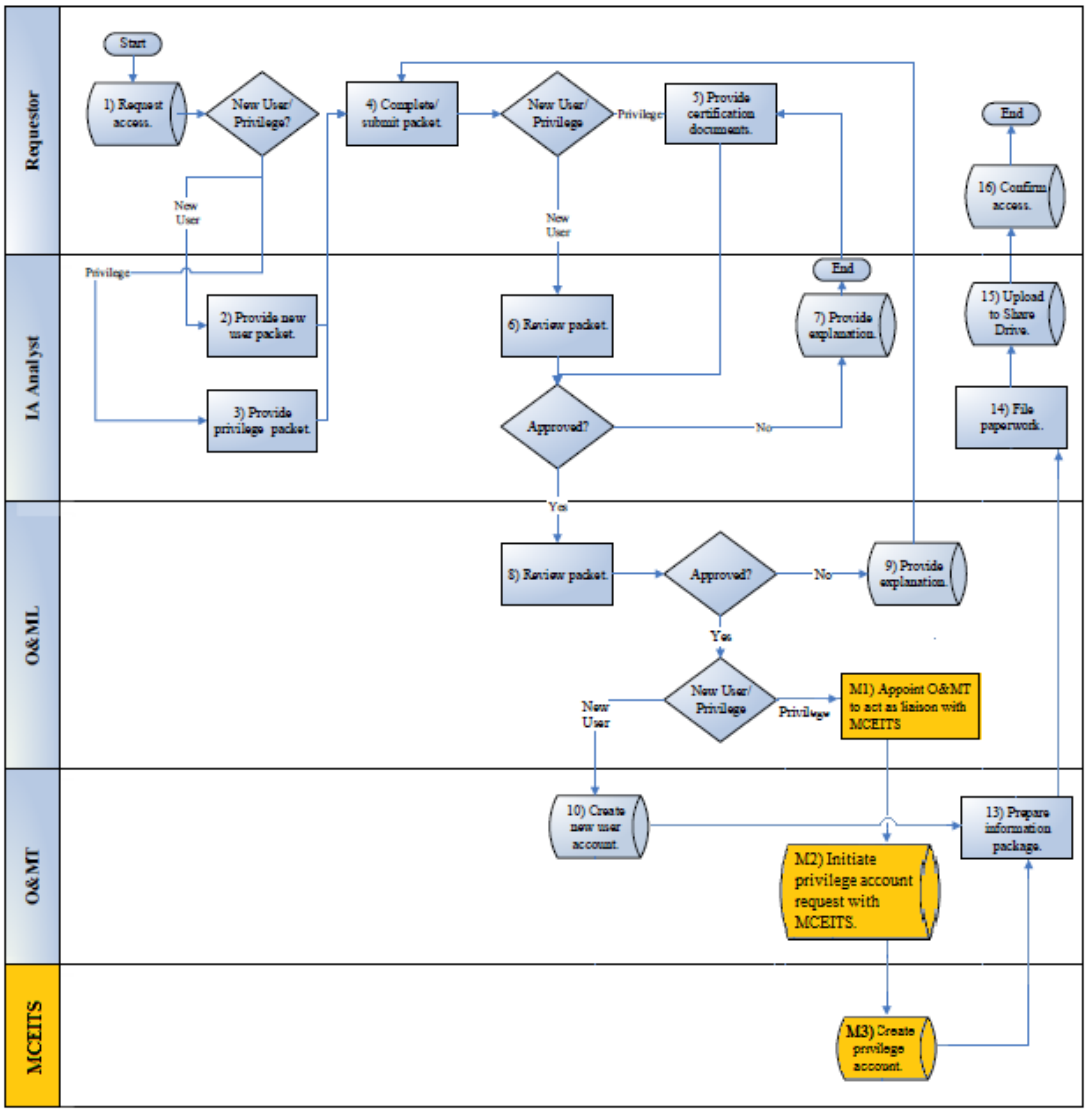


Table 15. Proposed Access Control – User Accounts Process Step-by-Step Description

Step	Activity Details
1	Requestor notifies or concludes that access to the LMS domain is needed for specific task-related activity, and requests access be granted. If the new account is for a standard user, proceed to Step 2. If the new account is for a privileged (i.e., administrative) account, proceed to Step 3.
2	Remedy notifies the IA Analyst of the request. The IA Analyst provides the new account packet that includes forms and required reading material.
3	Remedy notifies the IA Analyst of the request. The IA Analyst provides **privilege** account packet that includes forms and required reading material.
4	The Requestor reviews the provided materials, completes the application/training, and submits the packet to the IA Analyst. If the individual is a new user, proceed to Step 6. If the individual will receive a privilege account, proceed to Step 5.
5	The Requestor provides certification documentation to the IA Analyst.
6	The IA Analyst reviews the completed packet and determines whether to grant the request. If the IA Analyst grants the request, proceed to Step 8, otherwise go to Step 7.
7	The IA Analyst provides a written explanation of the reason for denial of the request. Return to Step 5.
8	O&ML reviews the completed packet and accompanying documentation. If the O&ML denies the request, proceed to Step 9. If the OM&L approves the request for a new user and the new user is a standard user, proceed to Step 10. If the approval is for a privilege user, proceed to Modified Step 1.
9	O&ML closes the Remedy ticket after documenting the denial justification. Return to Step 4.
10	O&ML assigns the account creation to an O&MT member who then creates the account. Proceed to Step 13.
M1	[New Step] O&ML assigns an O&MT member to open to act as a liaison (point of contact) with MCEITS for establishing the privilege account.
M2	[New Step] O&MT initiates the privilege account creation request with MCEITS customer support. The O&MT will provide MCEITS with documentation as required.
M3	[New Step] MCEITS customer support creates the privilege account and assigns permissions.
13	O&MT prepares and sends the IA Analyst a “welcome packet” for the new account holder.
14	The IA Analyst files the account creation paperwork in the local Share Drive.
15	The IA Analyst loads the request documentation to the Share Drive.
16	The Requestor receives the Information Package from the IA Analyst including the credential information and uses the NOC to access the domain with the login information. The process ends.

The first modification after Step 8, when the Operations and Maintenance Lead (O&ML) determines if the new account request is for a standard user account or a privileged account. If the request is for a standard user account, then the remaining process flow is unchanged. For a privileged account request, the process flow moves to Step, M1, where the O&ML assigns an Operations and Maintenance Team (O&MT) member to act as a point of contact with MCEITS. At Step, M2, the assigned O&MT member initiates a privilege account creation request with MCEITS customer support and provides any required documentation. At Step, M3, MCEITS customer support creates the privilege account, assigns permissions, notifies the O&MT point of contact, and closes the request in Remedy. After Step M3, the process will follow the same flow through Steps 13 through 15 from the original process.

b. Incident Reporting and Handling Process

The questions regarding the post-migration Incident Reporting and Handling Process involved who control the response to a reported security issue or incident. According to Mark Johnson (telephone interview, November 20, 2015), ultimate responsibility for incident reporting lies with the application owner. Therefore, the DLNOC will implement the Incident Reporting and Handling Process.

Due to its interaction with the MCEITS datacenter, the Incident Reporting and Handling Process will require some minor modifications after the migration. The proposed changes to the process flow diagram and process description appear in Figure 21 and Table 16, respectively.

Figure 21. Proposed Incident Reporting and Handling Process

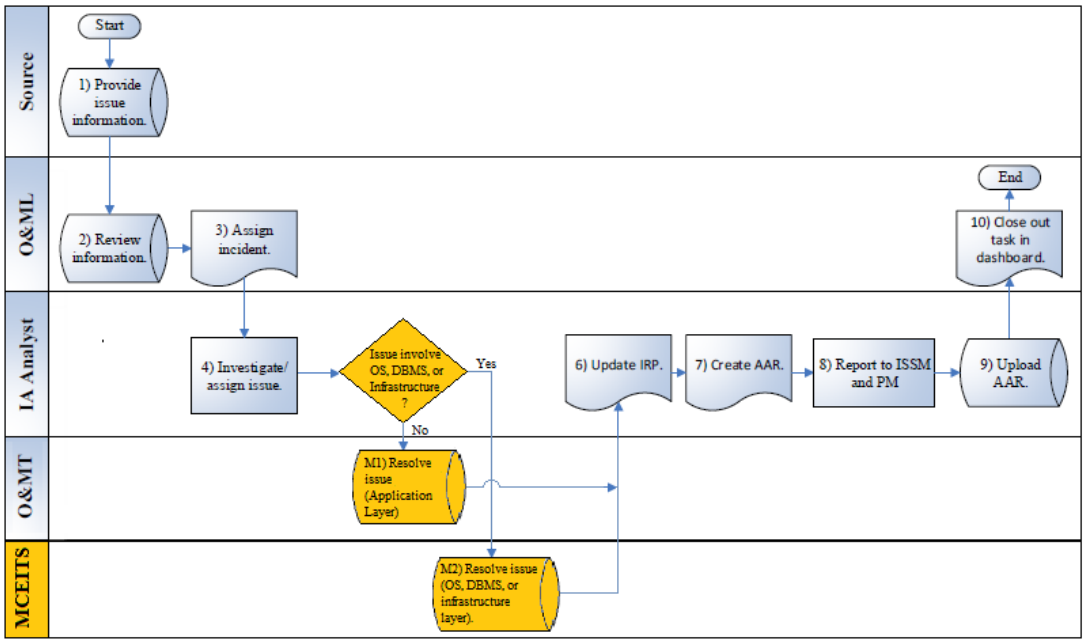


Table 16. Proposed Incident Reporting and Handling Process Step-by-Step Description

Step	Activity Details
1	The Source provides information about an issue by opening a ticket in Remedy.
2	Remedy forwards the issue to the O&ML who reviews the information and documents the issue in the tasking dashboard.
3	The O&ML assigns the ticket to an IA Analyst.
4	The IA Analyst conducts an investigation. If the issue involves the server operating systems (OS), DBMS, or the infrastructure (physical hardware), the IA Analyst contacts MCEITS. Otherwise the IA Analyst creates resolution options and then assigns the issue to the O&MT to perform necessary corrective actions.
M1	[Modified Step] O&MT resolves the Application Layer issue and returns it to the IA Analyst.
M2	[New Step] MCEITS resolves the OS, DBMS, or infrastructure issue and closes service request ticket/notifies IA Analyst.
6	The IA Analyst updates the Incident Response Plan (IRP).
7	The IA Analyst creates an After Action Report (AAR).
8	The IA Analyst sends the AAR to the Information Security System Manager and the Program Manager (PM).
9	The IA Analyst uploads the AAR to the share drive for future reference.
10	The O&ML then closes the ticket in Remedy.

The first modified step occurs at Step 4, where the Information Assurance (IA) Analyst investigates the reported security issue. If the issue does not involve the server OS, DBMS, or other MCEITS infrastructure, then the IA Analyst assigns the issue to the O&MT for resolution. At Step, M1, which replaces the original Step 5, the O&MT resolves the issue at the Application Layer and provides information to the IA Analyst at Step 6. If the issue does involve the server OS, DBMS, or other MCEITS infrastructure, then the IA Analyst will contact MCEITS customer support for resolution. At the Step, M2, MCEITS customer support resolves the issue, closes the service request ticket, and provides information to the IA Analyst for updating the Incident Response Plan (IRP). From Steps 6 through 10, the process remains unchanged.

c. Compliance Reporting Process

Like the incident reporting and handling, the compliance with all security notices and reviews are the final responsibility of the application owner (M. Johnson, telephone interview, February 11, 2016). As a result, the Compliance Reporting Process will require similar changes as those presented for the Incident Reporting and Handling Process. The proposed Compliance Reporting Process has modification steps in it to address times when MCEITS customer support will need to be involved in addressing a compliance issue. However, the DLNOC should rarely have to contact MCEITS with compliance issues because MCEITS has its own internal compliance process (M. Johnson, telephone interview, February 11, 2016). MCEITS are required to review security notices every 30 days, but they normally do compliance reviews weekly (M. Johnson, telephone interview, February 11, 2016). The proposed Compliance Reporting Process, presented in Figure 22 and Table 17, contains modifications for the rare times that a compliance issue involves MCEITS resolution.

Figure 22. Proposed Compliance Reporting Process

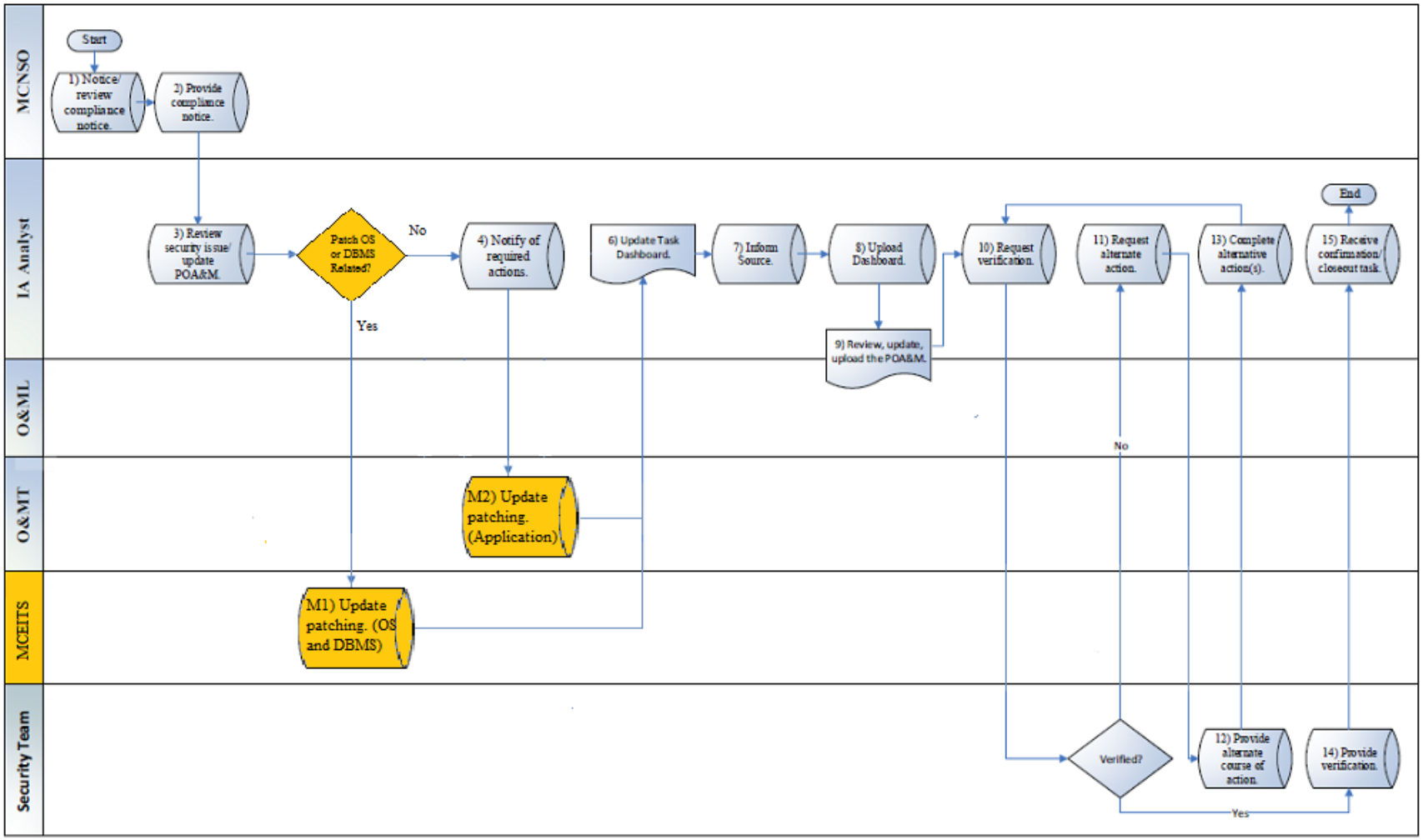


Table 17. Proposed Compliance Reporting Process Step-by-Step Description

Step	Activity Details
1	The Marine Corps and Navy Security Officer (MCNSO) notices and reviews the security notice(s).
2	The MCNSO provides the IA Analyst the security notice(s) and opens a Remedy ticket.
3	The IA Analyst reviews vulnerabilities, security changes requested/needed, determines the patches required and steps to address security needs, makes a resource assignment, and documents the POA&M and the ticket. If the patch involves the OS, DBMS, or is otherwise MCEITS related, contact MCEITS customer support (Step M1). Otherwise, assign the issue to the O&MT (Step M2).
4	The IA Analyst notifies O&MT of the completed research and required patching.
M1	[New Step] MCEITS updates patching on the OS and DBMS Layer, as required, and notifies IA Analyst when task is complete.
M2	[Modified Step] O&MT completes the patching on the Application Layer.
6	The IA Analyst updates the Task Dashboard (i.e., a tracking sheet) and closes the ticket.
7	The IA Analyst informs the Source of the resolution.
8	The IA Analyst uploads the Task Dashboard to the Marine Corps Standard Patching and Incident Reporting SharePoint (SIPR SP).
9	O&ML meets with the IA Analyst to prepare and update/upload the POA&M to mitigate future security issues.
10	The IA Analyst requests a Security Team verification. If compliance is verified, proceed to Step 14. Otherwise, proceed to Step 11.
11	The IA Analyst requests an alternative course of action from the Security Team.
12	The Security Team provides an alternate course of action.
13	The IA Analyst completes the alternative action(s). Return to Step 10.
14	The Security Team verifies compliance and provides the IA Analyst verification.
15	The IA Analyst receives approval and instructions to close out the security issue from the Security Team. The process ends.

In the proposed process, after Step 3 the IA Analyst determines if the security patch concerns the OS, DBMS, or MCEITS infrastructure. If this proves to be the case, the IA Analyst contacts MCEITS customer support via service request who installs patching as required in Step, M1. After M1, MCEITS customer support reports the patch completion to the IA Analyst at Step 6. If at Step 3 the IA Analyst determines that the issue pertains to the application layer, the IA Analyst proceeds to Step 4 and notifies the O&MT. At Step M2 (originally Step 5 from the original process) the O&MT patches the application layer and then informs the IA Analyst at Step 6. The rest of the process from Steps 6 through 15 remains the same as the original process.

2. Database Administrator Functions

Changes to the Database Administrator functions will require modification depending on the degree of interaction with the database. After the migration, the DLNOC personnel will have administrative rights to the database and retain ownership of the database application software (S. Gibson, personal interview, February 12, 2016). However, the DBMS will itself will be under MCEITS's control. Any process that requires manipulation of the DBMS or the database itself would require MCEITS customer support assistance (S. Gibson, personal interview, February 12, 2016). The Database Administrator functions will require modification to reflect this change in database ownership.

a. Ad Hoc/Canned Reporting Process

The Ad Hoc/Canned Reporting Process involves using database applications to interact with the DBMS in order to generate reports. The process does not require making alterations to the DBMS or database itself. Therefore, the proposed process will work the same as the original process. The modifications in the proposed process are meant to address the rare occasions when CDET's database application is not able to generate the requested report. Under such a scenario, the DLNOC may be able to request the needed database application software from MCEITS (S. Gibson, personal interview, February 12, 2016). MCEITS will provide access to application software already in its software portfolio (S. Gibson, personal interview, February 12, 2016). However, if MCEITS does

not have access to the requested application software, then the DLNOC may have to initiate the Procurement Process to acquire it. Figure 23 and Table 18 contains the diagram and details, respectively, for the proposed Ad Hoc/Canned Reporting Process.

Figure 23. Proposed Ad Hoc/Canned Reporting Process

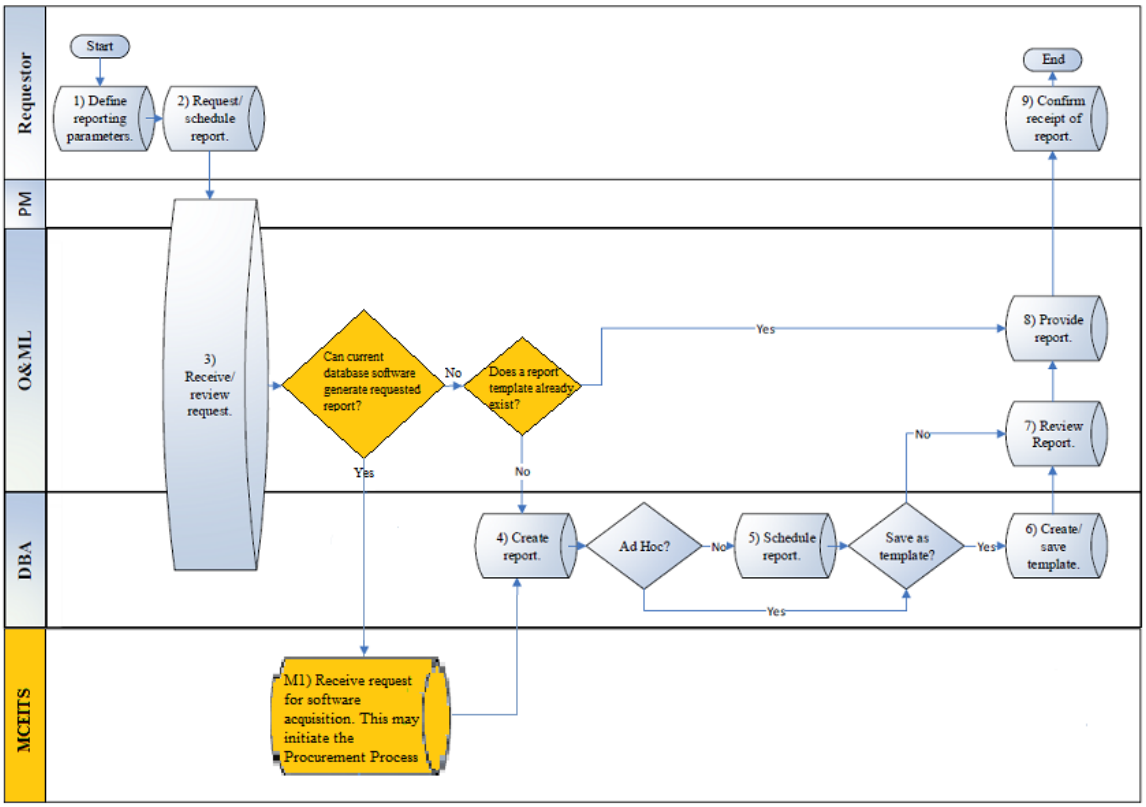


Table 18. Proposed Ad Hoc/Canned Reporting Process Step-by-Step Description

Step	Activity Detail
1	The Requestor defines the specific reporting parameters required for the report.
2	A Requestor contacts the Program Manager (PM), O&ML, or Database Administrator (DBA) and requests a customized report.
3	The O&ML, PM, or DBA receives the request for an ad hoc report. The OM&L and DBA will determine if the current software applications can generate the requested report. If report requires new software, place a request with MCEITS (M1). Otherwise, the O&ML and DBA will review the request together and determine whether or not an existing template will fulfill the reporting parameters. If a template exists, proceed to Step 8. If there is no existing template, proceed to Step 4.
M1	[New Step] MCEITS receives request for software to interact with the DBMS to provide the requested report. If MCEITS does not have access to the required software, MCEITS may direct the DBA to initiate the Procurement Process.
4	The DBA creates the report and determines whether or not to save the report as a template. If the report is to be a "canned" report, proceed to Step 5. If the report is to be an ad hoc report, determine whether the report is to be saved as a template. If it is to be saved as a template, proceed to Step 6. If the "canned" report is not saved as a template, proceed to Step 7.
5	The DBA schedules the new report to generate according to the schedule outlined in the report's parameters.
6	The DBA saves the report as a template.
7	O&ML reviews the customized report. If the report is acceptable, proceed to Step 8. If the report is unacceptable, return to Step 4.
8	O&ML submits the customized report to the Requestor.
9	The Requestor receives the customized report from the O&ML and confirms receipt. The process ends.

The first modification appears at Step 3 after the Program Manager (PM), O&ML, or DBA receives the request for a report. The PM, O&ML, or DBA with determine if CDET's current database application software can fulfill the request. If the current database application software is adequate, then the process will flow in the same way as the original process. If CDET's database application software is not adequate, then the PM, O&ML, or DBA will place a request with MCEITS customer support to acquire the needed software. At Step M1, MCEITS will provide the software if available. However, Step M1 provides a warning that initiation of the Procurement Process may be necessary if the requested software is not part of the MCEITS portfolio.

b. Database/System Restore (Zone A)

The Database/System Restore Processes are for restoring the database to a previous state. For this analysis, the assumption is that "restoring" the database would require access to backup data. Under the PaaS model, manipulation of data storage, the DBMS, and the database itself falls to MCEITS. Therefore, Database/System Restore processes with require considerable MCEITS participation.

Within MCEITS, the Zone A environment functions as the Stage environment. Therefore, the proposed Database/System Restore (Zone A) Process will replace the Database/System Restore (Stage) Process. Since Zone A is a test environment and the restore process would not affect CDET's customers, the DBA may initiate the process without O&ML approval (Booz Allen Hamilton, 2015). From the CDET DLNOC perspective, the proposed process has less complexity since MCEITS is responsible for more of the actual work involved. Figure 24 and Table 19 provide the diagram and details for the process, respectively.

Figure 24. Proposed Database/System Restore (Zone A) Process

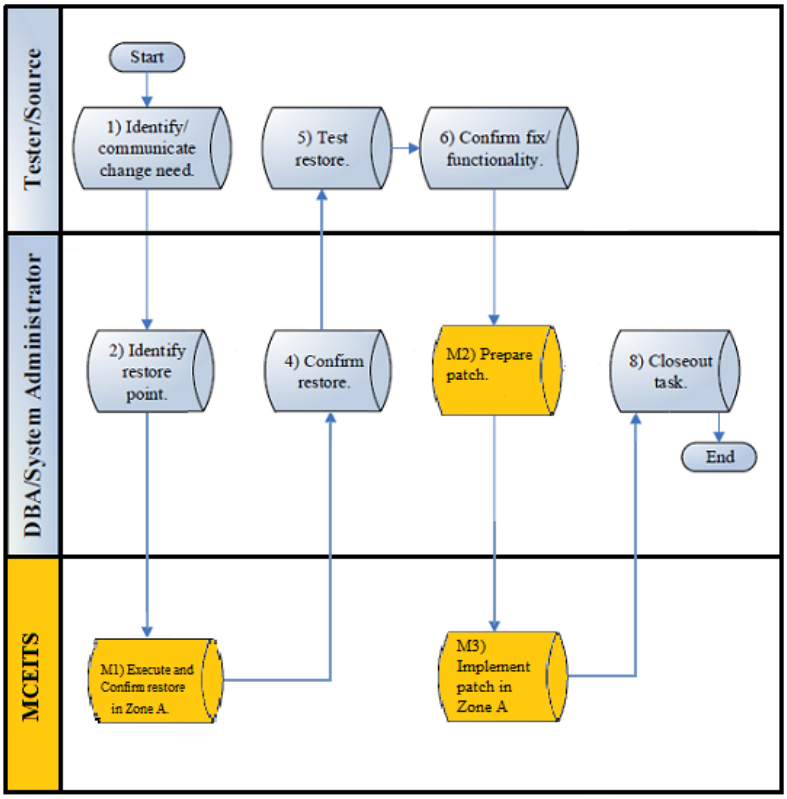


Table 19. Proposed Database/System Restore (Zone A) Step-by-Step Description

Step	Activity Detail
1	The Tester or other Source identifies the need for a change in the database or system. If a database change is required, the Tester informs the DBA. If a system change is required, the system administrator is informed. When the Tester identifies a need, he/she opens a ticket in Remedy.
2	The DBA or System Administrator identifies the restore point and initiates a MCEITS service request.
M1	[New Step] MCEITS executes and confirms the restore in Zone A.
4	The DBA or System Administrator confirms the restore took place in Zone A
5	The Tester determines (i.e., tests) whether or not the data was restored in Zone A.
6	The Tester confirms that the "fix" in the database/system restored all functionality in Zone A.
M2	[Modified Step] The DBA or System Administrator prepares the patch and provides it to MCEITS.
M3	[New Step] MCEITS implements the patch in Zone A.
8	The DBA or System Administrator closes out the task in the dashboard, and closes the ticket.

The first modification occurs at Step 2, when the DBA or System Administrator identifies the restore point. After the migration, the DBA or System Administrator will need to initiate a MCEITS customer support request to restore the database or system in the Zone A environment. Under Step M1, MCEITS customer support executes and confirms the restore. Any difficulties encountered during the restore process are the responsibility of MCEITS customer support where it was the responsibility of the DBA or System Administrator under the original process. After the DBA or System Administrator confirms MCEITS restore (Step 4), the Tester tests the restore and confirms a fix (Steps 5 and 6). Under Step M2, the DBA or System Administrator prepares the patch and provides it to MCEITS for implementation at Step M3. Once MCEITS customer support completes the patch implementation, the DBA or System Administrator closes the task at Step 8.

c. Database/System Restore Process (Production)

Since, the Database/System Restore Process (Production) requires the coordination of a system outage, it requires approval of the O&ML (Booz Allen Hamilton, 2015). Accordingly, the proposed Database/System Restore Process (Production) involves greater interaction between the O&ML and MCEITS. Again, the assumption is “restoring” the database requires accessing data from the MCEITS backup system. The diagram and step-by-step description for the proposed process appear in Figure 25 and Table 20, respectively.

Figure 25. Proposed Database/System Restore Process (Production)

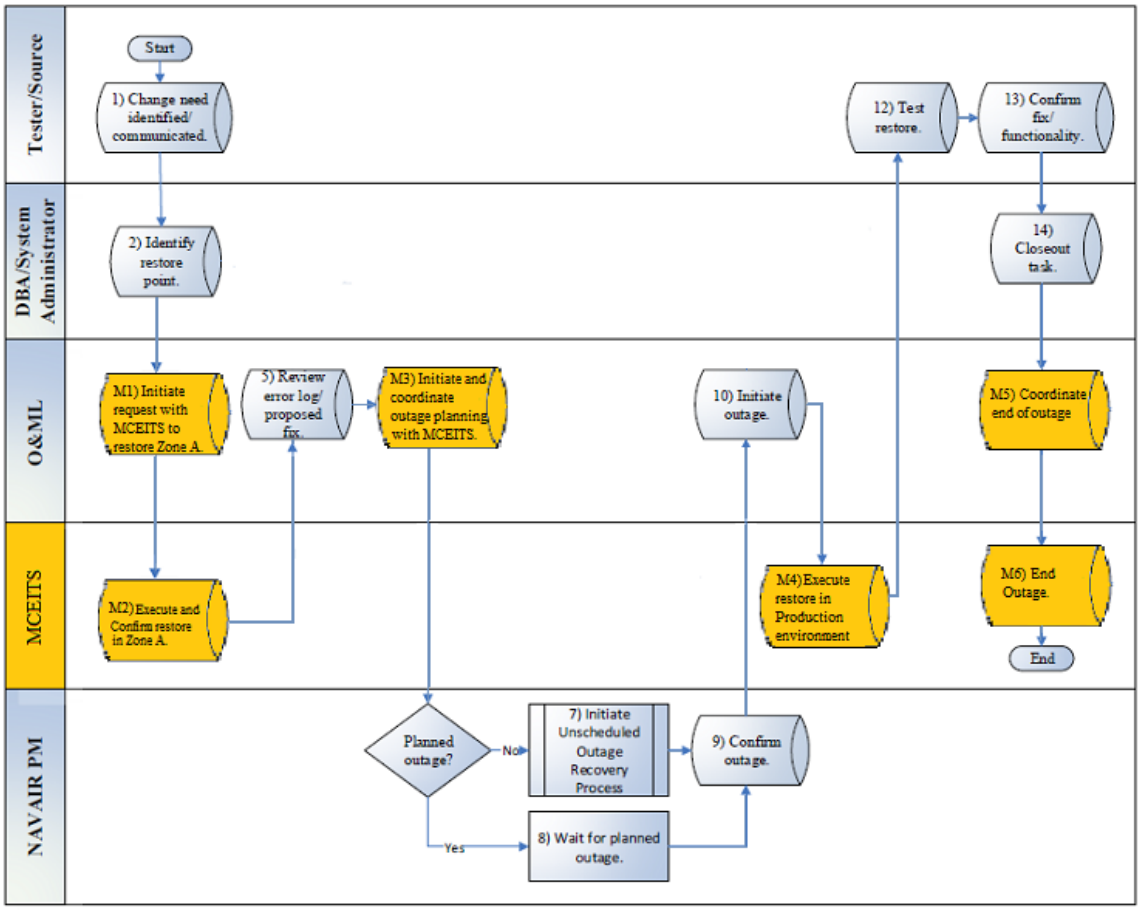


Table 20. Proposed Database/System Restore Process (Production) Step-by-Step Description

Step	Activity Details
1	The Tester identifies the need for a change in either the database or system and notifies the DBA if a database change is required or the System Analyst if a system change is required.
2	The DBA or System Analyst receives notification of the database/system and identifies the restore point.
M1	[Modified Step] The O&ML initiates a service request with MCEITS to restore Zone A to the identified restore point.
M2	[New Step] MCEITS executes and confirms the Zone A restore.
5	O&ML reviews the error log and the proposed fix.
M3	[Modified Step] O&ML initiates the outage planning in coordination with MCEITS. If the fix can wait until the next planned outage, proceed to Step 7. If the fix cannot wait until the next planned outage, proceed to Step 8.
7	O&ML initiates the Unscheduled Outage Recover Process.
8	The NAVAIR PNM waits until the next scheduled outage for the affected system.
9	The NAVAIR PM confirms the outage schedule with CDET.
M4	[Modified Step] O&ML initiates outage at the schedule time/date and requests MCEITS execute the restore in the Production environment.
12	The Tester assesses the restore in Production.
13	The Tester confirms the fix and functionality in Production and notifies the DBA or the System Administrator.
14	The DBA or the System Administrator closes out the task in the Task Dashboard and the ticket in Remedy.
M5	[Modified Step] O&ML coordinates the end of the outage.
M6	[New Step] MCEITS ends the outage. Process ends.

The proposed process begins in the same way as the original, but starts to differ at Step M1. When the O&ML receives the requested restore point, he or she will initiate a request with MCEITS to restore Zone A at Step M2. The purpose of restoring Zone A first is to ensure conformity for the Zone A and Production environments. After the restoration of Zone A, the O&ML reviews the error log and proposed fix (Step 5). At Step M3 (formerly Step 6 in the original process), the O&ML initiates and coordinates the outage planning process with MCEITS. The outage plan is then sent to and handled

by the Naval Air Systems Command (NAVAIR) PM at Steps 7, 8, and 9, in the same manner as the original process. Once the NAVAIR PM confirms the outage plan for the Production environment, the O&ML requests MCEITS to execute the database/system restore at Step M4. After the Production environment restore, the Tester tests the restore and confirms the fix (Steps 12 and 13) and the DBA/System Administrator closes the task (Step 14). At Step M5 (formerly Step 15), the O&ML coordinates with MCEITS to end the outage. The process then ends after MCEITS ends the outage at Step M6.

d. Monthly Backup Offsite Process

According to the *Marine Corps Enterprise Information Services (MCEITS) Information Technology (IT) Standards Guide Version 2.0* (Colangelo, 2015), MCEITS provides a Backup and Recovery process for data protection services. MCEITS's process utilizes Storage Area Network (SAN) based backups for its virtual machines and traditional agent-based backups for physical and database systems (Colangelo, 2015). The process saves the backups initially to a near-line storage system (HP StoreOnce 6500) and then to offline tape storage system (MSL6480 Tape Library) (Colangelo, 2015). According to MCEITS Services Integrated Product Team (IPT) Lead, Mark Johnson (telephone interview, November 20, 2015), MCEITS has a standard periodicity for conducting backups; however, CDET may negotiate more frequent backups as part of the SLA.

Since MCEITS provides this Backup and Recovery process, the DLNOC will no longer need to conduct its Monthly Backup Offsite Process. Keeping the Monthly Backup Offsite Process within DLNOC would create unnecessary redundancy and added expense. Therefore, the recommendation is to completely eliminate the Monthly Backup Offsite Process from the DLNOC SOP guide.

3. Hosting and Network

With the Stage and Production environments migrating to virtual servers, the processes under the Hosting and Network functional area will require modifications to address this new operational model. Changes to network configurations, patch and release management, and outage recovery will all require coordination between the

DLNOC and MCEITS. The following proposed processes will attempt to address this operational shift.

a. Change Request Process

The original Change Request Process existed to address the physical server environment at the DLNOC. After the migration to MCEITS, the servers in the Production or Zone A environments will be virtual servers whose configurations will be under the control of MCEITS. Changes to the network configuration will require significant interaction with MCEITS customer support. The proposed Change Request Process appears in Figure 26 and Table 21.

Figure 26. Proposed Change Request Process

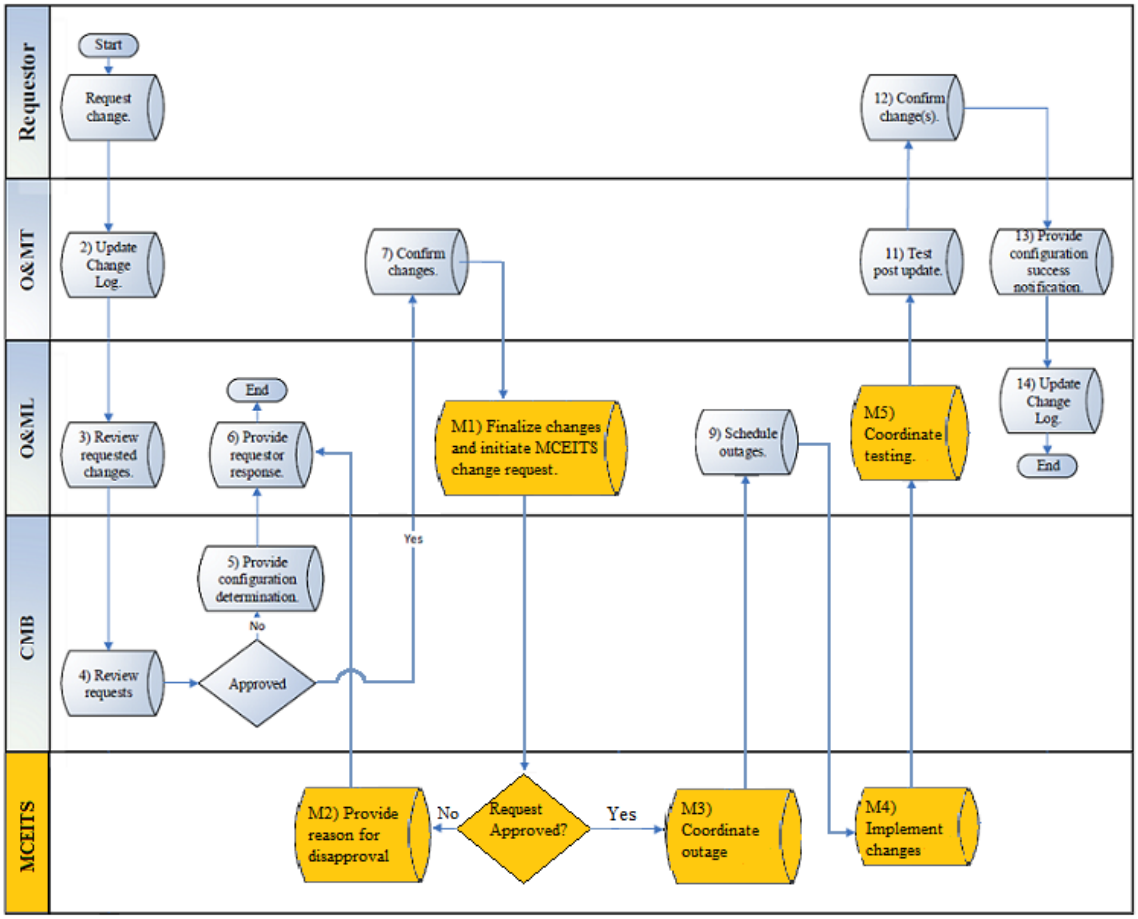


Table 21. Proposed Change Request Process Step-by-Step Description

Step	Activity Detail
1	The Requestor identifies the need for a configuration change and requests it.
2	O&MT receives the request and updates the DLNOC Change Log.
3	O&ML facilitates a meeting with O&MT to review each requested configuration change.
4	The Configuration Management Board (CMB) reviews each configuration change request and determines whether or not to honor the request. If the request is not honored, proceed to Step 5. If the request is honored, proceed to Step 7.
5	The CMB informs the O&ML of their decisions regarding the configuration request.
6	O&ML notifies the requestor of the denied configuration request. The process ends.
7	O&ML enters "CONFIRMED" in the change log to confirm the final configuration changes.
M1	[Modified Step] O&ML reviews the final configuration change(s) and initiates a change request with MCEITS customer support.
M2	[New Step] If MCEITS is unable to comply with the request, MCEITS denies the request and provides justification to O&ML.
M3	[New Step] If MCEITS approves the request coordinates the outage schedule with the O&ML.
9	O&ML creates schedules an outage that will be used to implement and notifies O&MT.
M4	[New Step] MCEITS implements the requested changes.
M5	[Modified Step] O&ML coordinates with MCEITS and O&MT for the testing of the implemented changes.
11	O&MT tests the update and notifies the Requestor when the testing is completed. Note: This step is referred to as a "high level smoke test."
12	Requestor checks the system changes to verify functionality/capability and reports findings to O&MT.
13	O&MT informs O&ML with confirmation of successful configuration change.
14	O&ML updates the Change Log and closes the process.

Steps 1 through 7 of the proposed process remains unchanged from the original. After confirming the requested changes at Step 7, the O&ML finalizes the changes and initiates a MCEITS change request at Step M1 (formerly Step 8). When MCEITS customer support receives the change request, it must determine if MCEITS can accommodate the request. If it cannot, MCEITS will provide the reason for disapproval and send the request back to the O&ML (Step M2). If MCEITS approves the request, it will coordinate the system outage with the O&ML (Step M3). After the O&ML schedules

the outage (Step 9), MCEITS will implement the changes at Step M4. At Step M5, the O&ML will coordinate testing the changes with MCEITS and the O&MT. After successful testing of the changes, the new process will conclude with Steps 11 through 14 in the same way as the original process.

The proposed Change Request Process will be necessary only when major changes to the network configuration is necessary. Minor changes to the configuration, such as increased memory capacity or computing power, will not require a formal change request. As one of the benefits of cloud computing, MCEITS can dynamically allocate additional computing resources when needed (M. Johnson, telephone interview, November 20, 2015). In fact, MCEITS has system monitoring software that can detect when a customer's system needs increased resources and will automatically provide it (M. Johnson, telephone interview, November 20, 2015). THE DLNOC will initiate the proposed Change Request Process when a significant change is necessary (i.e., new server dedicated to a new application).

b. Patch Management Process

Patches to the OS, DBMS, or other MCEITS infrastructure is the responsibility of MCEITS. When MCEITS technicians receive notification of an available patch, the standard practice is to apply the patch in the Zone A environment and then wait one week before applying to the Production environment (M. Johnson, telephone interview, February 11, 2016). This is done to verify that a patch will not adversely affect the customers' applications. If a customer discovers an issue with a patch, it can request that MCEITS not apply the patch to the Production environment. However, if the patch is security related, the customer will need to develop a mitigation plan and request approval from Headquarters, Marine Corps Command, Control, Communications and Computers (HQMC C4).

Regarding patches applied to application level software, the Patch Management Process will remain relatively unchanged. The proposed process, shown in Figure 27 and Table 22, indicates the steps to take in the rare event that the DLNOC discovers an OS, DBMS, or other MCEITS infrastructure patch not implemented by MCEITS.

Figure 27. Proposed Patch Management Process

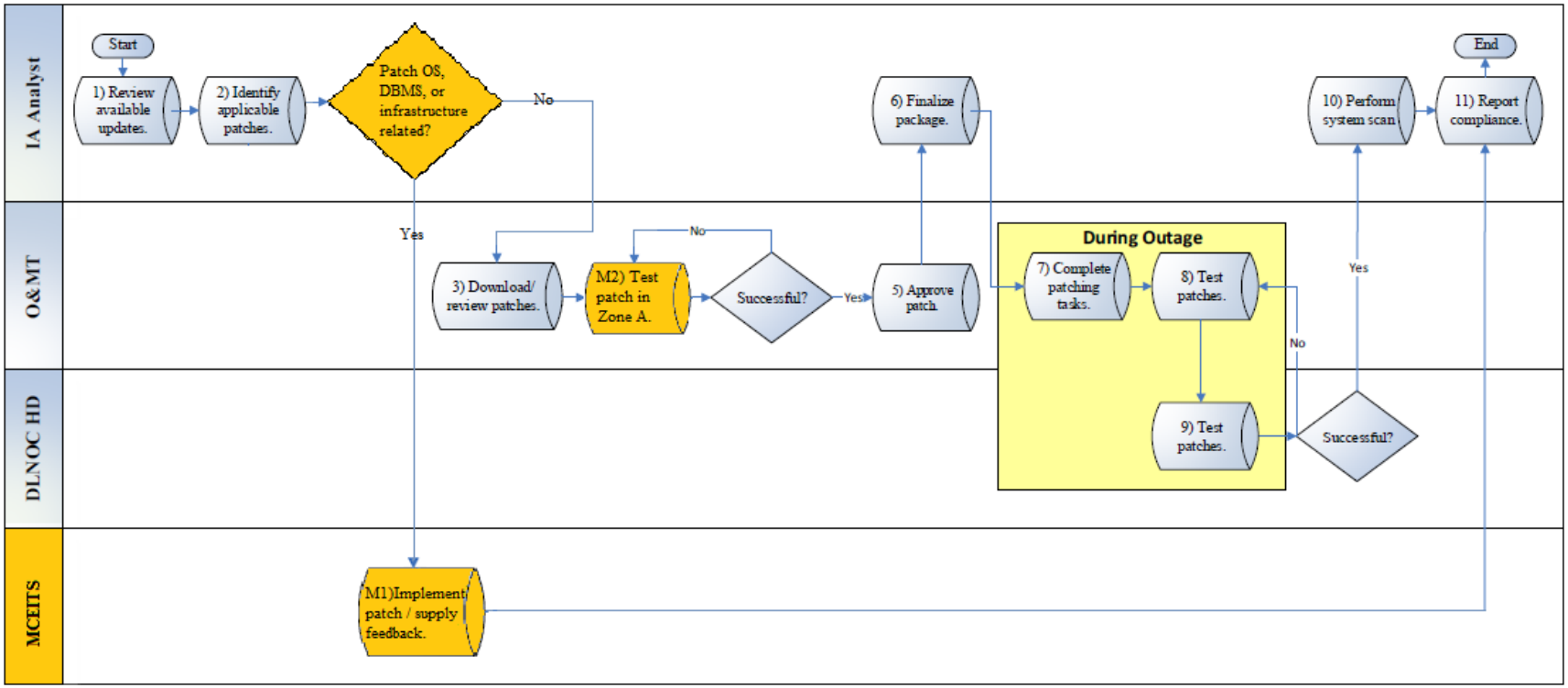


Table 22. Proposed Patch Management Process Step-by-Step Description

Step	Activity Detail
1	The IA Analyst reviews the available Microsoft (MS) updates.
2	The IA Analyst identifies the applicable patches. If the patch involves the OS, DBMS, or other MCEITS provided infrastructure, then contact MCEITS (Step M1). Otherwise, assign task to the O&MT (Step 3).
M1	[New Step] MCEITS implements the patch and supplies feedback. Process ends.
3	O&MT downloads, reviews, and packages the applicable patches.
M2	[Modified Step] O&MT tests the patch in the Zone A environment. If the test is successful, proceed to Step 5. If the test is not successful, return to Step M2.
5	O&MT approves the patch to be installed during the IA outage.
6	The IA Analyst finalizes the patch package to be implemented during the IA outage.
7	O&MT completes all of the patch activities.
8	O&MT tests the patch in Production and notifies the DLNOC Help Desk (HD) when their test is completed. Note: The testing process is documented and placed on the Shared Drive. This test is also referred to as a "smoke test." Often a ticket is opened for this step in Remedy, and it is assigned to the O&ML. When a second level of testing is completed, the O&ML re-assigns the ticket to the DLNOC HD. Testing results are documented and this step is completed during an IA outage.
9	DLNOC HD repeats the patch testing and documents the testing results in the Remedy ticket. If the testing is not successful, repeat Step 8. If the testing is successful, update/close the ticket and proceed to Step 10. This step is completed during an IA outage.
10	The DLNOC IA System Analyst performs a full system scan. Note: This scan process is fully documented and available of the Shared Drive.
11	DLNOC IA System Analyst reports the compliance based upon the scan results to the original initiator. The process ends.

After the IA Analyst reviews and identifies an applicable update/patch (Steps 1 and 2), he or she must then determine if the patch applies to the OS, DBMS, or other MCEITS infrastructure. If the update is indeed MCEITS related, then the IA Analyst will contact MCEITS customer support. MCEITS will then apply the patch (Step M1) and provide feedback to the IA Analyst at Step 11. If the IA Analyst determines the patch

applies at the application level, the process will proceed in the same manner as the original Patch Management Process. The only change would be at Step M2 (originally Step 7) that specifies that patch testing will occur in Zone A. This change ensures that Zone A replaces “Stage” in the process description.

c. LMS Release Management Process

The LMS software is specific to the application layer of the PaaS model and will remain in the full control of CDET. As a result, the proposed LMS Release Management Process contains only minor recommended changes. Figure 28 and Table 23 shows the flow diagram and step-by-step description, respectively.

Figure 28. Proposed LMS Release Management Process

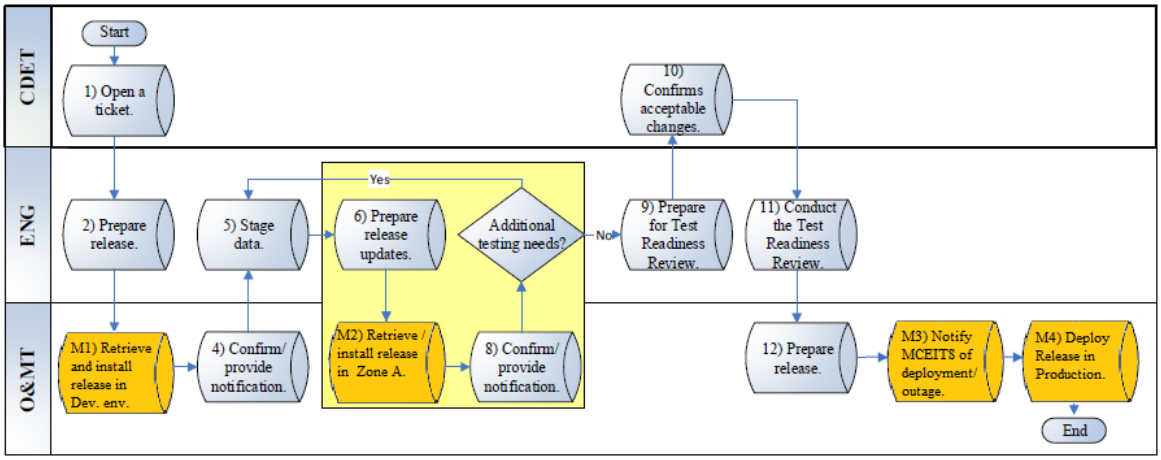


Table 23. Proposed LMS Release Management Process Step-by-Step Description

Step	Activity Detail
1	CDET opens a ticket to initiate the LMS release.
2	DLNOC Engineering Team (ENG) prepares a development release for Production.
M1	[Modified Step] O&MT retrieves the release and installs it in the Development environment.
4	O&MT confirms the release and provides an installation notification.
5	ENG stages the data.
6	ENG prepares additional release updates.
M2	[Modified Step] O&MT retrieves/installs release in Zone A.
8	O&MT confirms the release and provides an installation notification.
9	ENG prepares for the Test Readiness Review.
10	CDET confirms that the changes are acceptable.
11	ENG conducts the Test Readiness Review.
12	O&MT prepares the release for Production.
M3	[New Step] Notify MCEITS of LMS deployment/outage (courtesy).
M4	[Modified Step] O&MT deploys the release to Production, ending the process.

Step M1 modifies the original Step 3 so that the O&MT installs the software release in the Development environment for testing. Steps 4, 5, and 6 remain unchanged from the original process. Step M2 is a modified version of Step 7 in which the O&MT retrieves the release from the Development environment and installs it into the Zone A environment. Steps 8 through 12 remain unchanged. At Step M3, the O&MT provides a courtesy notification to MCEITS to inform them of the pending LMS deployment and outage. The DLNOC should provide this courtesy so that MCEITS customer support can respond to any service calls it should receive due to the outage. Step M4, which replaces Step 14, specifies that the final release's installation in the Production environment and O&MT brings the system back online.

d. Outage Scheduling Process

After the migration, the O&ML will retain primary responsibility for maintaining the system outage schedule. CDET and MCEITS will negotiate the initial outage schedule during migration planning (M. Johnson, telephone interview, February 11, 2016). However, the DLNOC will still need to have an Outage Scheduling Process for making changes to the schedule. During a system outage, MCEITS often receives numerous calls to its customer support help desk, regardless of whether the outage is MCEITS caused (M. Johnson, telephone interview, February 11, 2016; S. Gibson, personal interview, February 12, 2016). Providing the MCEITS customer support with an outage script would help with dealing these calls. The proposed Outage Scheduling Process provides additional steps to implement this recommended coordination. Figure 29 and Table 24 present the proposed Outage Scheduling Process.

Figure 29. Proposed Outage Scheduling Process.

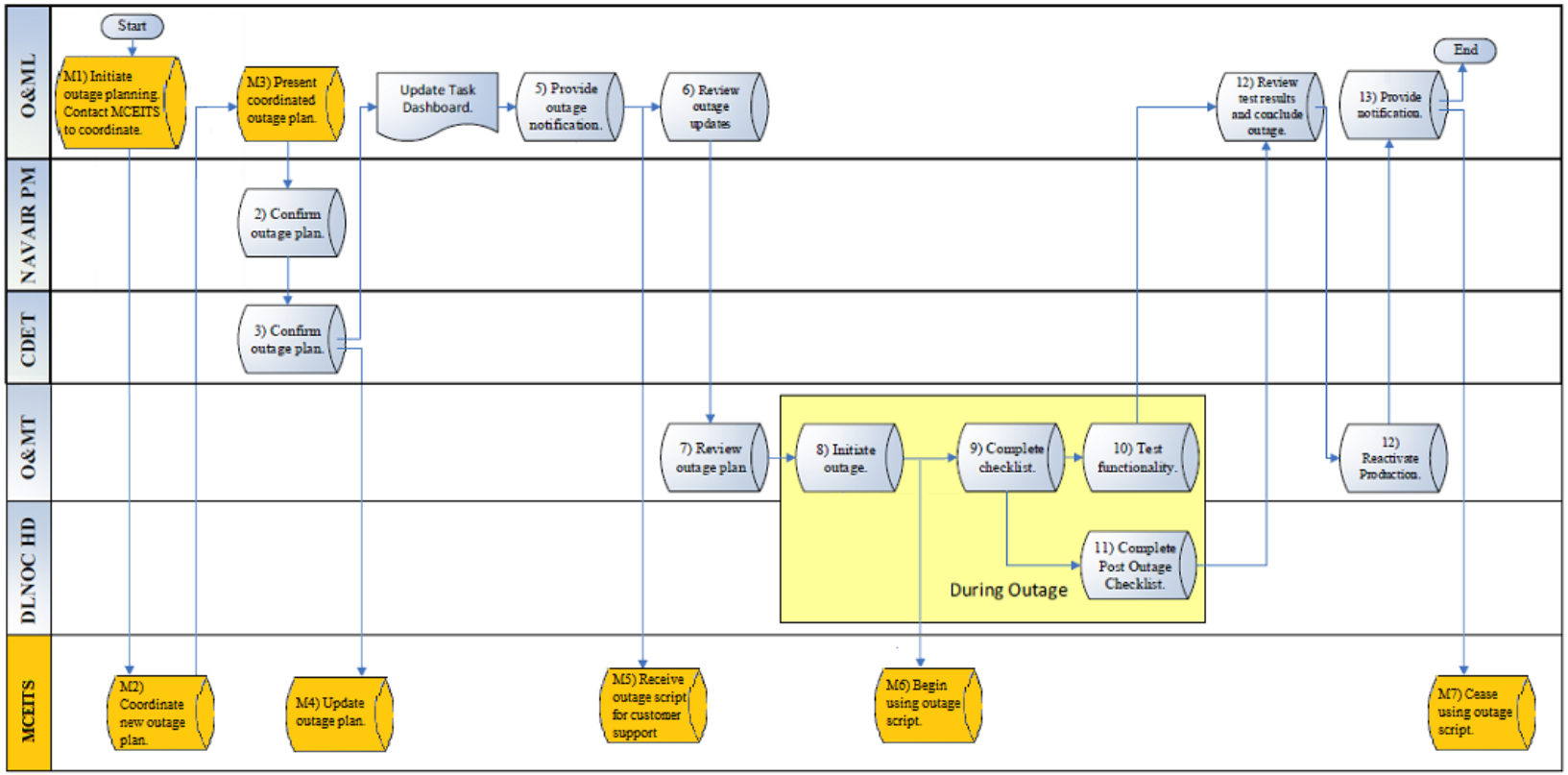


Table 24. Proposed Outage Scheduling Process Step-by-Step Description

Step	Activity Detail
M1	[Modified Step] O&ML initiates outage planning and contacts MCEITS to coordinate.
M2	[New Step] MCEITS works with O&ML on new outage plan.
M3	[New Step] O&ML informs NAVAIR PM of the new outage plan.
2	The NAVAIR PM confirms the outage plan and notifies CDET.
3	CDET confirms the outage plan and notifies the O&ML and MCEITS.
M4	[New Step] MCEITS updates its outage plan with the approved changes.
4	O&ML assigns a resource to the outage and updates the Task Dashboard with the resource information.
5	O&ML notifies the LMS stakeholders of the outage events. Also, O&ML provides MCEITS with an outage script for its customer support desk.
M5	[New Step] MCEITS customer support desk receives the outage script for use during outages.
6	O&ML reviews the outage updates.
7	O&MT the outage plan.
8	O&MT initiates the outage per the outage schedule and informs MCEITS customer support to begin using the outage script.
M6	[New Step] MCEITS customer support begins using the outage script.
9	O&MT completes the activities that are outlined in the Outage Checklist.
10	O&MT tests the affected system's/LMS's functionality and confirms.
11	The DLNOC Help Desk completes the Post Outage Checklist (POC) and notifies the DLNOC O&M.
12	O&MT reactivates LMS in Production and concludes the outage.
13	O&ML notifies stakeholders that the outage has ended and the next scheduled outage via email. MCEITS customer support is informed of the end of the outage. The process ends.
M7	[New Step] MCEITS customer support stops using the outage script.

The proposed process begins with Step M1 in which the O&ML initiates the outage planning and contacts MCEITS to coordinate. At Step M2, MCEITS works with the O&ML to develop the new outage plan. At Step M3, the O&ML notifies the NAVAIR PM of the new outage plan. The NAVAIR PM confirms the new outage plan and informs CDET at Step 2. After CDET confirms the plan at Step 3, CDET notifies the

O&ML and MCEITS of the approved plan. MCEITS updates its copy of the outage plan at Step M4. After the O&ML provides outage notification at Step 5, the O&ML provides MCEITS customer support with an outage script at Step M5. After the initiation of the outage at Step 8, MCEITS receives the notice to start using the outage script at Step M6. For the last modification at M7, MCEITS customer support ceases using the outage script after reactivation of the Production environment.

e. Unscheduled Outage Recovery Process

Unscheduled outages due to a MCEITS issue will normally trigger an internal MCEITS process (M. Johnson, telephone interview, February 11, 2016). In that scenario, MCEITS would be the source that informs the DLNOC while simultaneously executing the outage recovery process.

When dealing with an unscheduled outage of undetermined cause, the O&ML will need to include MCEITS in the investigation and recovery process. There may be times when an outage is MCEITS related but MCEITS customer support is unaware of the issue. Therefore, coordination with MCEITS is a necessary modification for the post-migration unscheduled outage response. The proposed Unscheduled Outage Recovery Process contains changes to allow for this coordination. The flow diagram for the proposed process appears in Figure 30; a step-by-step description is shown in Table 25.

Figure 30. Proposed Unscheduled Outage Recovery Process

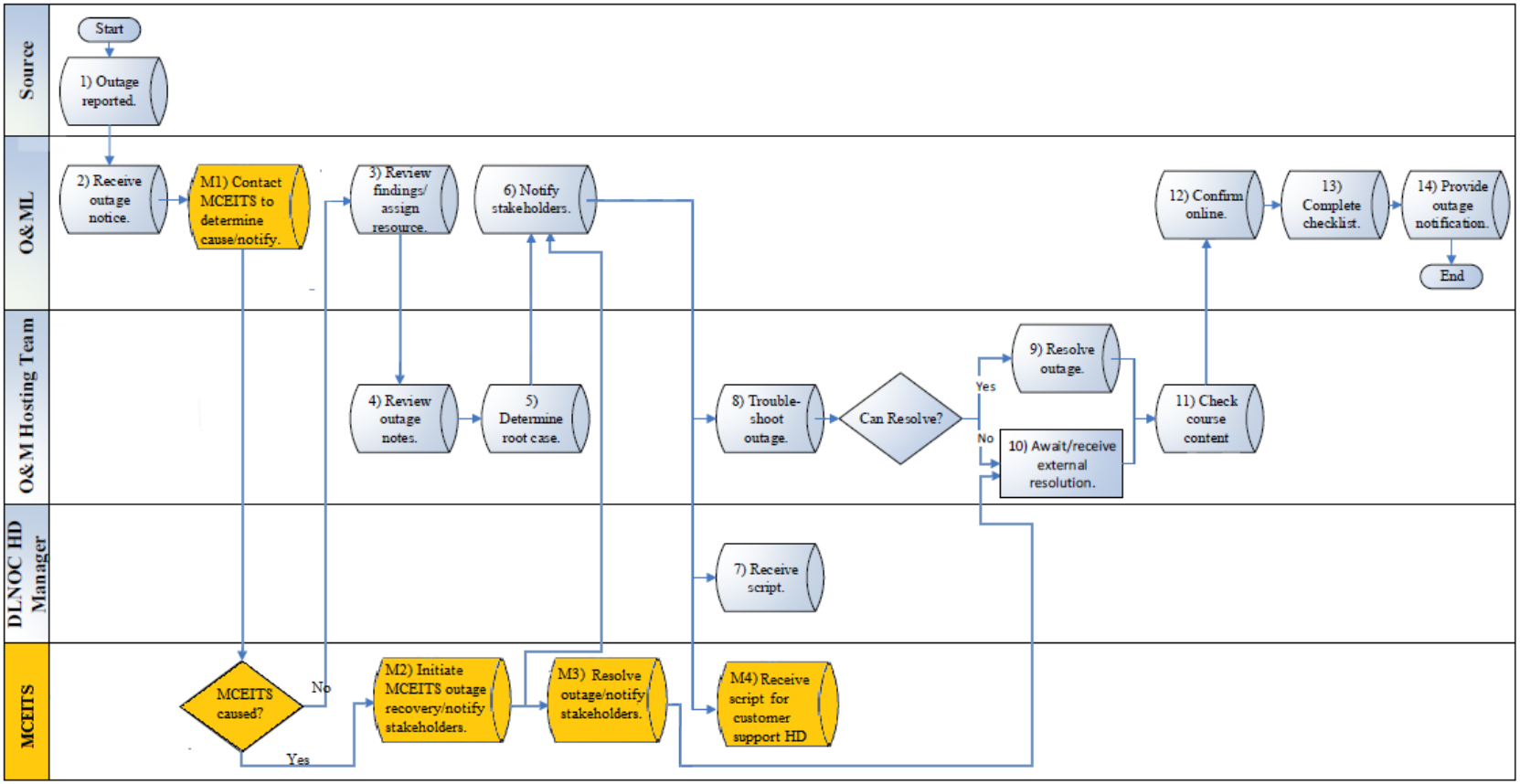


Table 25. Proposed Unscheduled Outage Recovery Process

Step	Activity Detail
1	A Source notifies the O&ML of a possible outage via an automated report or through and increase in Help Desk tickets.
2	O&ML receives the outage notification.
M1	[New Step] O&ML contacts MCEITS to determine if the outage is MCEITS related. If the outage is MCEITS related, MCEITS initiates internal outage recovery process (Step M2). Otherwise, proceed to Step 3.
M2	[New Step] MCEITS initiates outage recovery process and notifies all stakeholders (Step 6). Proceed to Step M3.
M3	[New Step] MCEITS resolves the outage, notifies stakeholders, and proceeds to Step 10.
3	O&ML reviews outage findings and assigns a resource to the outage.
4	O&M Hosting Team of the affected system review the outage notes.
5	O&M Hosting Team determines the outage's root cause.
6	O&ML notifies the affected system's stakeholders to the root cause.
M4	[New Step] MCEITS customer support receives the script to share with callers regarding an unplanned outage.
7	DLNOC Help Desk Manager receives the script to share with callers regarding an unplanned outage.
8	O&M Hosting Team troubleshoots outage or awaits external resolution. If the incident can be resolved, proceed to Step 10. If the incident cannot be resolved, proceed to Step 9.
9	O&M Hosting Team resolves the outage.
10	O&M Hosting Team receives resolution from external sources.
11	O&M Hosting Team checks the LMS course content.
12	O&ML confirms that the LMS is online and available to use.
13	O&ML completes the Scheduled Outage Checklist.
14	O&ML provides stakeholders an outage status notification. The process ends.

After receiving notification of an outage (Step 2), the O&ML should contact MCEITS customer support (Step M1) to make it aware of the outage and determine if the cause is MCEITS related. If the outage is not MCEITS related (i.e., no other MCEITS customers are affected), then the process will continue in the same manner as the original

Unscheduled Outage Recovery Process. If the outage is MCEITS related, the process flows to Step M2 where MCEITS customer support initiates its internal outage recovery and notifies its stakeholders, including the DLNOC (at Step 6). At Step M3, MCEITS resolves the issue and notifies its stakeholders of the resolution.

The last addition to the process occurs after the O&ML notifies its stakeholders of the outage. When the O&ML provides the DLNOC Helpdesk with an outage script for responding to phone calls (Step 7), MCEITS customer support should also receive the script (Step M4) to answer calls that it receives from CDET customers.

4. Administration

After the migration, the O&ML will maintain primary responsibility for the administrative functions for the DLNOC. The following proposed processes will show how the O&ML will interact with MCEITS when executing the Tasking Process and Procurement Process.

a. Tasking Process

After the migration, tasks needing MCEITS customer support will require DLNOC personnel to submit a service request via MCEITS's Remedy service management system. DLNOC personnel will not be able to task MCEITS personnel directly. The changes to the proposed Tasking Process diagram and step-by-step description appear in Figure 31 and Table 26, respectively.

Figure 31. Proposed Tasking Process.

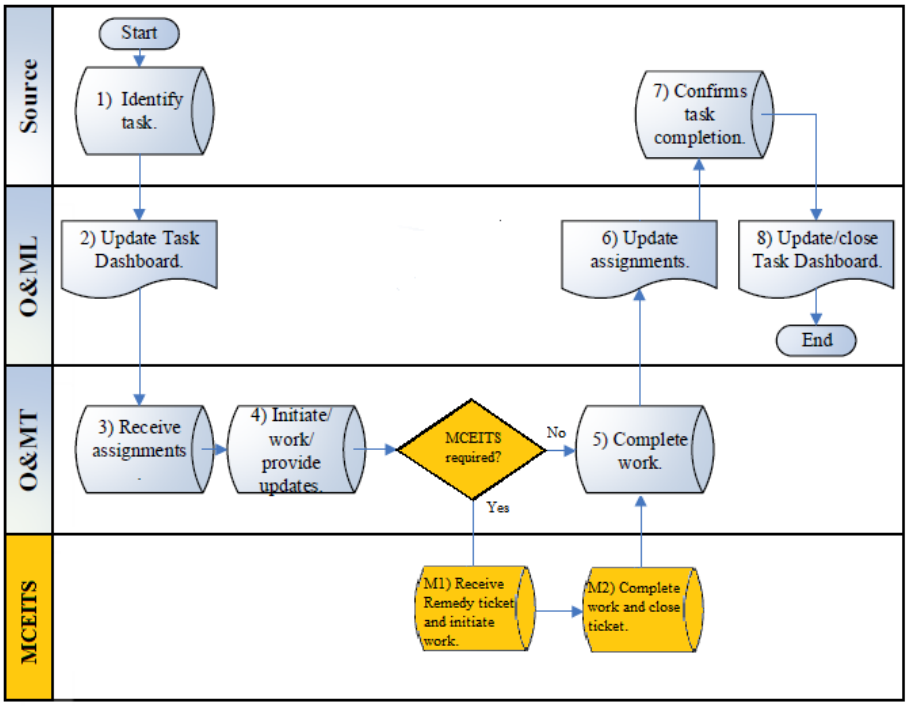


Table 26. Proposed Tasking Process Step-by-Step Description

Step	Activity Detail
1	A Source identifies a task for the O&MT and informs the O&ML.
2	O&ML adds the task information including tasks and resource assignments to the Task Dashboard that is maintained on the Shared Drive.
3	O&MT receives the tasks and task assignments in person, email, and/or Remedy.
4	O&MT begins the work per the assignment. All information regarding the status of the task is updated in the ticket details. If the task requires MCEITS involvement, the initiate a trouble ticket with MCEITS customer support, record the MCEITS ticket number in the original ticket details, and proceed to Step M1. Otherwise, proceed to Step 5.
M1	[New Step] MCEITS receives service request ticket and processes it in accordance to its priority.
M2	[New Step] MCEITS completes work, closes ticket, and notifies O&MT.
5	O&MT completes the task per the assignment and closes the corresponding ticket.
6	O&ML updates assignments to load balance the workload.
7	Source confirms to the O&MT or O&ML that the task has been completed.
8	The O&ML closes the tasking in the Task Dashboard. The process ends.

After initiating work on the assigned task (Step 4), the O&MT determines if the task requires assistance from MCEITS customer support. If the O&MT does not need MCEITS customer support to complete the task, then the proposed Tasking Process continues in the same manner as the original process. If the O&MT does need MCEITS customer support, the O&MT submits a service request and records service request number in the original DLNOC ticket. MCEITS receives the service request at Step M1, assigns it a priority level, and initiates work on the task (Step M1). After MCEITS customer support completes the work on the task, it closes out the service request and notifies the O&MT (Step M2). Steps 5 through 8 are unchanged from the original process.

b. Procurement Process

The Procurement Process will not change for DLNOC's acquisition for application level software and hardware for the Development environment. However, the process will be different for procuring changes to the MarineNet logical network within MCEITS. Procuring additional servers will simply require a MCEITS change request since the servers are virtual and not physical. As previously mentioned, a benefit of cloud computing is the ability to dynamically allocate new computing resources. As long as the change request involves a service or resource that MCEITS can provide (i.e., additional servers, DBMS, increased memory, or additional computing power), MCEITS will approve the request. The changes within the MCEITS hosting environment should not incur any additional costs to CDET (M. Johnson, telephone interview, February 11, 2016).

Figure 32. Proposed Procurement Process

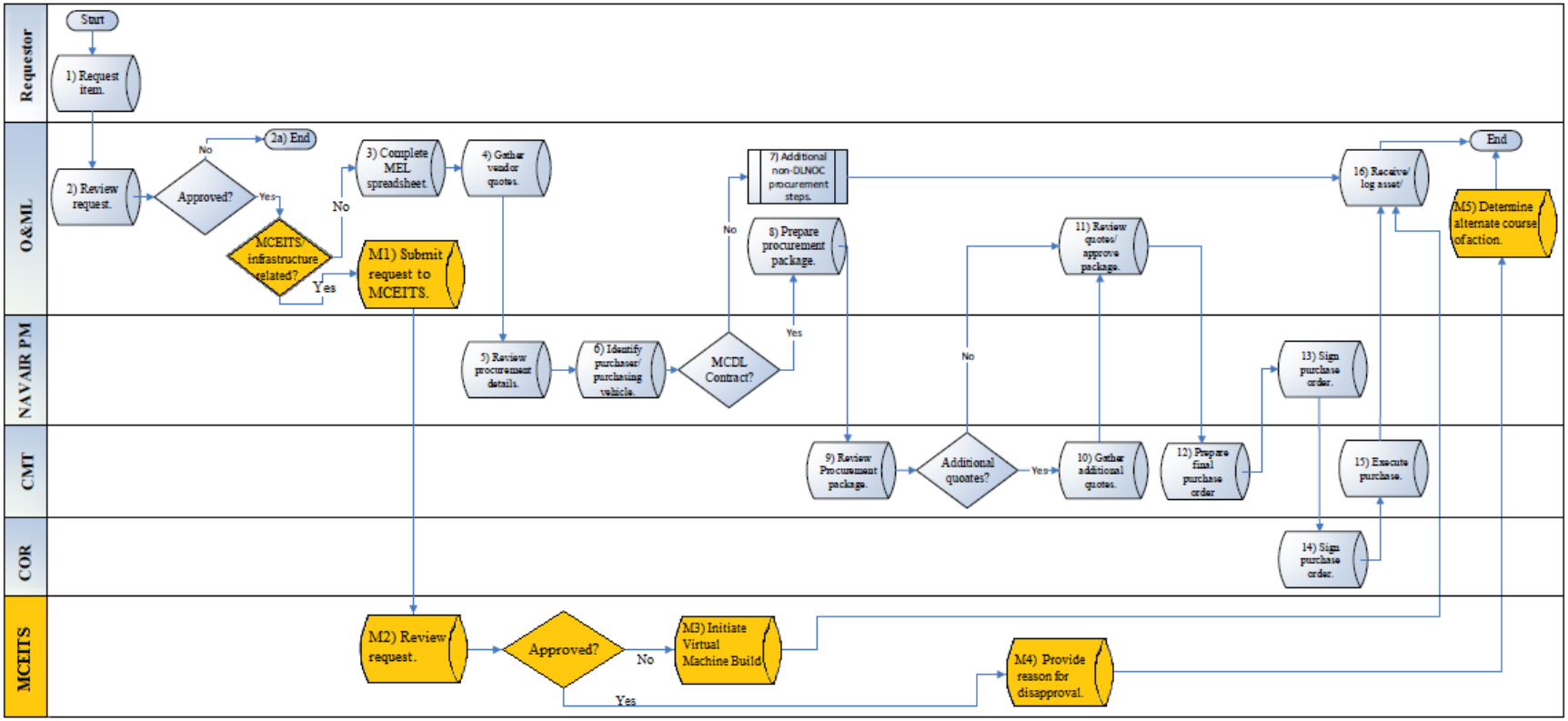


Table 27. Proposed Procurement Process Step-by-Step Description

Step	Activity Detail
1	Requestor asks for a specific asset that requires procurement and includes the justification for the asset.
2	The O&ML reviews the request and justification. If O&ML denies the request, O&ML provides the reason for the denial and the process ends. If the request is approved, determine if the request requires additional capabilities from MCEITS. If the request does not involve MCEITS, proceed to Step 3. If request requires MCEITS involvement, proceed to Step M1.
M1	[New Step] Submit request to MCEITS.
M2	[New Step] MCEITS reviews the request. If the request is approved, proceed to Step M5. Otherwise, proceed to Step M3.
M3	[New Step] MCEITS initiates Virtual Machine build and notifies O&ML when complete. Proceed to Step 16.
M4	[New Step] MCEITS provides reason for disapproval and notify O&ML (at Step M6).
M5	[New Step] O&ML determines alternate course of action. Process ends.
3	O&ML completes the MEL spreadsheet, which is available on the Shared Drive.
4	O&ML requests and collates pricing quotes from a minimum of 3 vendors.
5	The NAVAIR PM will review vendor quotes as prepared by the O&ML including cost estimate, delivery timeline, and support (if applicable) prior to selecting a funding vehicle.
6	NAVAIR PM identifies the purchaser and the purchasing vehicle to be used. If the contracting vehicle to be used is the Marine Corps Distance Learning (MCDL) contract, proceed to Step 8. If the contracting vehicle to be used is not the MCDL contract, determine if additional quotes are required. If additional quotes are needed, proceed to Step 10. If additional quotes are not needed, proceed to Step 11.
7	DLNOC staff has no further actions to take until the asset is received.
8	O&ML prepares the procurement package.
9	O&ML reviews the quotes and the procurement package and grants the package approval. If additional quotes are required, proceed to Step 10. If no additional quotes are required, proceed to Step 11.
10	Contract Management Team (CMT) obtains additional quotes per the O&ML's direction.
11	O&ML will review the draft procurement package including any additional vendor quotes received by the Material Team. This step insures that item(s) to be procured will meet the final need or intended need of the initial requestor.
12	CMT prepares the final purchase order.
13	NAVIAR PM reviews and signs the final purchase order. NAVAIR PM then provides the signed purchase order to the Contract Officer Representative (COR).
14	COR reviews and signs the final purchase order that has been signed by the NAVAIR PM.
15	CMT confirms the approval of the asset and places the purchase.
16	O&ML receives the new asset and logs the asset. The process ends.

Steps M1 through M5 describe the general process MCEITS would follow upon receiving a request for additional resources. After approving the request for additional resources from MCEITS, the O&ML will submit at request to MCEITS customer support. MCEITS will then review the request at Step M2. If MCEITS approves the request, then the virtual machine build will proceed (Step M3) and the O&ML will receive notification when the build is complete (Step 16). If MCEITS disapproves the request, MCEITS customer support will provide the reason for disapproval (Step M4) to the O&ML. At Step M5, the O&ML will then consider alternatives and the process ends. There are generally two reasons that MCEITS would disapprove a request. The first reason is that the request does not provide adequate details for completion (M. Johnson, telephone interview, February 11, 2016). In this circumstance, the O&ML would simply have to resubmit the request with the needed details. The other reason is that the request asks for capabilities beyond what MCEITS can provide (M. Johnson, telephone interview, February 11, 2016). If that is the case, then the O&ML would have to consider alternatives to the request.

C. SUMMARY

The diagrams and descriptions presented in this chapter are meant to be general depictions of how current DLNOC processes will change after the migration to MCEITS. They do not represent the definitive final processes, but rather they are meant to provide the CDET DLNOC with a basis of understanding for the impending changes. Any concerns not addressed by these proposed processes should become part of the SLA negotiations during the Preparation and Migration Planning phases of the MCEITS Application Inclusion Process.

Development of additional processes may be required to address some new issues created by the MCEITS migration. As previously mentioned, maintaining software synchronization across the Production, Zone A, and Development environments is a key concern when developing new software releases or troubleshooting problems that may arise. A dedicated process to ensure software synchronization is prudent. With MCEITS performing and maintaining all data backups, the DLNOC may wish to discuss a process

to allow access to that data should the need arise (for example, requesting backup data for use in the Development environment for troubleshooting purposes). Finally, there may be times when a software patch or release is larger that can be transferred using the standard VPN. A formal process to address this circumstance would be wise. These described processes should also be part of the SLA negotiations.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

Cloud computing is a concept that is changing the operating procedures of information technology (IT) departments everywhere. It promises to reduce costs by concentrating facility, equipment, and energy consumption expenses with the cloud service provider. Cloud service providers can provide their customers greater flexibility and scalability with current IT services, and allow for faster implementation of and access to new capabilities. Finally, customers that utilize cloud computing can let their IT departments focus on the specific needs of the organization while freeing them of the mundane tasks associated with maintaining a datacenter.

The federal government is seeking to incorporate cloud computing into its enterprise architecture because leaders see additional realizable benefits. Cloud computing can help streamline the acquisition process for IT hardware and software. This would be highly advantageous because cloud computing would allow the government to acquire IT as a service rather than purchasing physical hardware. Data center consolidation is another benefit because it decreases the number of entry points into federal networks, allowing for concentration of cyber security efforts. Finally, the federal government can have access to the latest industry best practices as supplied by the cloud service providers.

The Marine Corps Enterprise Information Technology Services (MCEITS) data center and hosting environment is the Marine Corps' program to implement private cloud computing into its enterprise architecture. It currently offers the Marine Corps' subordinate commands with Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) and will eventually offer Software as a Service (SaaS) as the capability is developed. MCEITS will provide "common hardware, software, and facilities infrastructure" that will enable "rapid collaboration, efficient discovery, and access to trusted data and information" for commands across the service (HQMC C4, 2012). This common environment will help with standardizing hardware and software while

improving security through the aforementioned data center consolidation. Additionally, MCEITS will allow its customer commands to quickly acquire additional computing resources through simple service change requests instead of dealing with the lengthy and cumbersome acquisition process for traditional network equipment. Furthermore, MCEITS will be meet its customers' need for increase resources proactively through its service monitoring capability.

Integral to MCEITS's success is overcoming the initial challenges of migrating Marine Corps' legacy systems to the MCEITS hosting environment. The first challenge of migration is ensuring that the customers will have the same IT capabilities that they had with their local data centers. Secondly, MCEITS must help their customers adapt their internal business processes in order to ensure necessary coordination takes place between the customers and the data center. Finally, MCEITS's must reassure the customer commands as they surrender the direct control they previously enjoyed over their systems. This reassurance will come as the customers embrace cloud computing technology and realize the advantages it offers.

As the College of Distance Education and Training (CDET) prepares for its migration, it must work with MCEITS to meet the previously mentioned challenges. The MCEITS Application Inclusion Process (AIP) describes the steps taken to assure that MCEITS will meet CDET's technical needs allowing CDET to maintain maximum control over its processes. As CDET adapts its processes to embrace MCEITS's cloud computing services,

B. FINDINGS

1. Research Question 1

Will the migration to the MCEITS environment require modifications to CDET's IT applications and systems and if so, will those modifications affect CDET's customer service?

As part of the AIP, the MCEITS team will work with CDET personnel to determine each application's suitability for migration. The migration will not occur until MCEITS can support CDET's application portfolio. Under MCEITS's PaaS service

model, it will provide the infrastructure (data center, storage, physical, and virtual servers), the operating systems, database, and applicable middleware for CDET to run its applications. CDET will maintain its applications. In the event that an application that is unable to run on the MCEITS supplied operating system or middleware, CDET may have to acquire the appropriate middleware and licensing. In the end, CDET should be able to run all its applications within the MCEITS hosting environment.

2. Research Question 2

Will the migration to the MCEITS environment require any significant changes to CDET's internal business processes? If so, which processes?

The "To-Be" processes presented in this thesis detail the potential modifications to the CDET Distance Learning Network Operation Center's (DLNOC) standard operating procedures needed to begin working in the MCEITS hosting environment. The primary basis for the modifications is the division of responsibilities after the migration. Processes that involve manipulating the MarineNet logical network below the application level face alteration to reflect MCEITS's required participation. Since all the processes described in the DLNOC Operations and Maintenance SOP involve interaction with the operating system, database management system (DBMS), or infrastructure, each process received an update to reflect the needed change.

Steps in the DLNOC processes that apply to the operation and maintenance of the locally retained Development environment will not change. Since MCEITS does not yet offer a Development environment for its customers, CDET will continue to manage a Development environment the same as it did before the migration.

3. Research Question 3

How can the requisite changes to CDET's business processes allow it to fully realize the benefits of cloud computing?

The most advantageous changes to CDET's business processes are those that previously involved dealing with the network infrastructure of MarineNet. After the migration, acquisition of additional computing resources for the Production and Zone A

environments will easier since CDET will rely on the Change Request Process instead of the Procurement Process. Furthermore, the CDET should see a much simpler Patch Management Process since software patches for the operating system, DBMS, and provided middleware is the responsibility of MCEITS. While the Database Restore Processes will require greater coordination between the organizations, MCEITS customer support will have the responsibility for most of the technical effort in the processes. Finally, CDET will be able to completely eliminate its Monthly Backup Offsite Process from its SOP manual since data backups is part of MCEITS standard services.

C. RECOMMENDATIONS

As stated in Chapter IV, maintaining software synchronization amongst the Production, Zone A, and Development environments is going to be key to for effective software development and testing. While MCEITS will have the responsibility for applying all server operating systems, databases, and middleware patches and updates, CDET's technicians must be aware of all the changes that MCEITS automatically applies. This will ensure that new software tested on one environment will work correctly in the other environments. Therefore, CDET should develop a process for tracking and validating synchronization.

Another recommendation is for CDET and MCEITS to establish an agreed upon terminology for addressing service request prioritization. When CDET submits a service request to MCEITS customer support, the two organizations should have an understanding of how the service requests are prioritized and how quickly work will be completed for a given priority. CDET and MCEITS should negotiate this terminology and provide it for inclusion in the Service Level Agreement (SLA).

Finally, CDET and MCEITS should establish liaisons/points of contact to facilitate better cooperation between the organizations. Having dedicated liaisons will help to quickly address any issues not foreseen or covered by the SLA.

D. FUTURE RESEARCH

As mentioned in Chapter IV, the “To-Be” diagrams and descriptions presented in this analysis are meant to proposed post-migration processes. After CDET completes the migration, future researchers could revisit this analysis and determine the accuracy of the proposed process modifications. Specifically, the researchers can ascertain if this analysis adequately predicted the challenges of the organizational adoption of cloud computing.

Since this analysis focused on organizational level adoption, another research opportunity would be to study cloud computing acceptance at the individual or community level. A survey of CDET employees after the migration may provide insight on how well they received and accepted the new technology. Do the employees like the new way of doing things? Has cloud computing lived up to its promised benefits from their perspective?

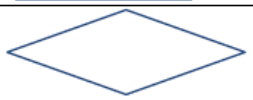
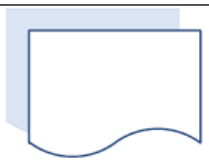
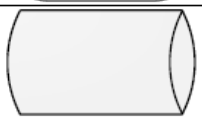
Finally, future researchers may want to continue to study MCEITS as it increases the services it provides. Will its customers adopt future services under development, such as, SaaS and virtual Development environments?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX

Figure 33 provides explanations for the symbology used in the process flow diagrams.

Figure 33. Process Flow Guide

Shape	Definition
	Denotes a task that is performed.
	Denotes a decision point within the process.
	Denotes a paper-based or electronic document or report.
	Denotes stored data.
	Denotes a process that is described in a separate process flow.
	Denotes the start/end of a process.
	Denotes a system where data is stored or manipulated.

Source: Booz Allen Hamilton. (2015). Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0. Quantico, MD: Naval Air Systems Command.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Anderson, R. (2012). *Marine Corps private cloud computing environment strategy.* Arlington, VA: U.S. Marine Corps Headquarters.

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58.

Buyya, R., Broberg, J., & Goscinski, A. (2011). *Cloud computing: Principles and paradigms.* Hoboken, NJ: John Wiley & Sons.

Booz Allen Hamilton. (2015). *Distance learning network operations center: Operations and maintenance standard operating procedure version 1.0* (Draft). Quantico, VA: Naval Air Systems Command.

Colangelo, D. (2015). *Marine Corps enterprise information services (MCEITS) information technology (IT) standards guide version 2.0.* Quantico, VA: Marine Corps Systems Command.

Davis, K., & Olson, D. (n.d.). *MCEITS 101* [PowerPoint]. Retrieved from https://mceits.usmc.mil/_layouts/PowerPoint.aspx

Department of Defense Chief Information Officer [DOD CIO]. (2013, September 18). *The Department of Defense strategy for implementing the Joint Information Environment.* Washington, DC: Department of Defense. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DoD_Strategy_for_Implmenting_JIE_(NDAA_931)_Final_Document.pdf

Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: Issues and challenges. *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, 27–33.

Grimes, J. (2007). *Department of Defense Net-Centric Services Strategy: Strategy for a Net-centric, Service Oriented DOD Enterprise.* Washington, D.C.: Department of Defense Chief Information Officer. Retrieved from http://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf

Headquarters Marine Corps Command, Control, Communications, and Computers [HQMC C4]. (2012). Marine Corps enterprise information technology services (MCEITS) [Web Page]. Retrieved from http://www.hqmc.marines.mil/Portals/156/Newsfeeds/SV%20Documents/Summaries/Marine%20Corps%20Enterprise%20IT%20Services.pdf

Headquarters Marine Corps Command, Control, Communications, and Computers [HQMC C4]. (2014). *Marine Corps Enterprise Network Unification Plan 2014–2017.* Retrieved from http://www.hqmc.marines.mil/Portals/156/Newsfeeds/SV%20Documents/MUP_v2_Mar2014.pdf

Kenyon, H. (2014, November 17). DoD changes cloud computing policy. *InformationWeek.* Retrieved from http://www.informationweek.com/government/cloud-computing/dod-changes-cloud-computing-policy/d/d-id/1317511

Khajeh-Hosseini, A., Greenwood, D., & Sommerville, I. (2010). Cloud migration: A case study of migrating an enterprise IT system to IAAS. *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on,* 450–457.

Kundra, V. (2011). *Federal cloud computing strategy*. Washington, DC: United States Chief Information Officer. Retrieved from http://acmait.com/pdf/Federal-Cloud-Computing-Strategy.pdf

Marine Corps Distance Learning Roadmap [MCDLR]. (n.d.). Retrieved from https://www.mcu.usmc.mil/cdet/docs/program/DLRoadmap.doc?mobile=0

Marrow, S. (2011). Data security in the cloud. In R. Buyya, J. Broberg, & A. Goscinski, (Eds.), *Cloud computing: Principles and paradigms* (pp. 573–592). Hoboken, NJ: John Wiley & Sons.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision support systems, 51*(1), 176–189.

Mehl, B. (2013). *MarineNet architecture design, version 1.0.* St. Inigoes, MD: Naval Air Systems Command Special Communications Requirements Division.

MITRE Corporation. (2000). *Functional requirements document (FRD) for the marine corps distance learning program learning management system (LMS).* Woodbridge, VA: The MITRE Corporation Quantico Site.

Mohan, T. (2011). Migrating into a cloud. In R. Buyya, J. Broberg, & A. Goscinski, (Eds.), *Cloud computing: Principles and paradigms* (pp. 43–56). Hoboken, NJ: John Wiley & Sons.

Olavsrud, T. (2015, July 13). Top cloud infrastructure-as-a-service vendors. *CIO*. Retrieved from http://www.cio.com/article/2947282/cloud-infrastructure/top-cloud-infrastructure-as-a-service-vendors.html#slide1

Rittinghouse, J. R. (2009). Cloud computing: Implementation, management, and security. Boca Raton, FL: CRC Press.

Schaefer, M. (2014). *MCEITS application inclusion process standard operating procedure* (OSS-210). Quantico, VA: Marine Corps Systems Command.

Sheldon, R. (2014, November 19). Data as a service: The next “as a service” wave? *Simple Talk.* Retrieved from https://www.simple-talk.com/cloud/cloud-data/data-as-a-service-the-next-”as-a-service”-wave/

Takai, T. (2012). *Cloud computing strategy.* Washington, DC: Department of Defense Chief Information Officer. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA563989

Tsai, W., Sun, X., & Balasooriya, J. (2010, April). Service-oriented cloud computing architecture. In *Information Technology: New Generations (ITNG), 2010 Seventh International Conference* (pp. 684-689). IEEE.

Welcome to CDET! [Web Page]. (n.d.). Retrieved from https://www.mcu.usmc.mil/cdet/SitePages/home.aspx

Yoo, C. S. (2011). Cloud computing: Architectural and policy implications. Review of Industrial Organization, *38*(4), 405 – 421. doi:10.1007/s11151-011-9295-7

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet services and applications,1*(1), 7–18.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California